



Ethernet Channel Configuration Guide IOS XE Release 3S (Cisco ASR 920 Series)

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

ITU-T G.8032 Ethernet Ring Protection Switching 1

Prerequisites for Configuring ITU-T G.8032 Ethernet Ring Protection Switching 1

About ITU-T G.8032 Ethernet Ring Protection Switching 1

Ring Protection Links 1

ITU-T G.8032 Ethernet Ring Protection Switching Functionality 2

R-APS Control Messages 2

CFM Protocols and Link Failures 3

G.8032 Ring-Supported Commands and Functionality 3

G.8032 ERP Timers 4

Protection Switching Functionality in a Single Link Failure and Recovery 5

Ethernet Flow Points 7

Service Instances and Associated EFPs 8

How to Configure ITU-T G.8032 Ethernet Ring Protection Switching 8

Configuring the Ethernet Ring Profile 8

Configuring Ethernet CFM MEPs 10

Enabling Ethernet Fault Detection for a Service 10

Configuring the Ethernet Protection Ring 12

Configuring Topology Change Notification Propagation 16

Configuring a Service Instance 17

Verifying the Ethernet Ring Protection (ERP) Switching Configuration 18

Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching 20

Example: Configuring Ethernet Ring Protection Switching 20

Example: Enabling Ethernet Fault Detection for a Service 21

Example: Verifying the Ethernet Ring Protection Configuration 22

CHAPTER 2

Configuring IEEE 802.3ad Link Bundling 23

Prerequisites for Configuring IEEE 802.3ad Link Bundling 23

Restrictions for Configuring IEEE 802.3ad Link Bundling 23

Information About Configuring IEEE 802.3ad Link Bundling	24
Gigabit EtherChannel	24
Port-Channel and LACP-Enabled Interfaces	24
IEEE 802.3ad Link Bundling	24
Benefits of IEEE 802.3ad Link Bundling	26
LACP Enhancements	26
LACP for Gigabit Interfaces	26
Features Supported on Gigabit EtherChannel Bundles	26
Guidelines for LACP for Gigabit Interfaces Configuration	28
How to Configure IEEE 802.3ad Link Bundling	29
Enabling LACP	29
Configuring a Port Channel	30
Configuring LACP (802.3ad) for Gigabit Interfaces	31
Setting LACP System Priority and Port Priority	34
Adding and Removing Interfaces from a Link Bundle	35
Removing a Channel Group from a Port	36
Setting a Minimum Threshold of Active Links	37
Monitoring LACP Status	38
Troubleshooting Tips	39
Displaying Gigabit EtherChannel Information	39
Configuration Examples for IEEE 802.3ad Link Bundling	44
Example: Configuring LACP for Gigabit Interfaces	44
Example Associating a Channel Group with a Port Channel	45
Example Adding and Removing Interfaces from a Bundle	46
Example Monitoring LACP Status	47
Example: Displaying Port-Channel Interface Information	48

CHAPTER 3**Multichassis LACP 49**

Prerequisites for mLACP	49
Restrictions for mLACP	50
Information About mLACP	51
Overview of Multichassis EtherChannel	51
Interactions with the MPLS Pseudowire Redundancy Mechanism	52
Redundancy Mechanism Processes	52
Dual-Homed Topology Using mLACP	53

LACP and 802.3ad Parameter Exchange	54
Port Identifier	54
Port Number	54
Port Priority	54
Multichassis Considerations	55
System MAC Address	55
System Priority	56
Port Key	56
Failure Protection Scenarios	56
Operational Variants	57
DHD-based Control	57
PoA Control	58
Shared Control (PoA and DHD)	58
mLACP Failover	58
Dynamic Port Priority	59
Revertive and Nonrevertive Modes	59
Brute Force Shutdown	59
Peer Monitoring with Interchassis Redundancy Manager	60
MAC Flushing Mechanisms	61
Multiple I-SID Registration Protocol	61
LDP MAC Address Withdraw	63
How to Configure mLACP	64
Configuring Interchassis Group and Basic mLACP Commands	64
Configuring the mLACP Interchassis Group and Other Port-Channel Commands	66
Configuring Redundancy for VPWS	67
Configuring Redundancy for VPLS	71
Coupled and Decoupled Modes for VPLS	71
Steps for Configuring Redundancy for VPLS	72
Configuring Hierarchical VPLS	76
Troubleshooting mLACP	80
Debugging mLACP	80
Debugging mLACP on an Attachment Circuit or EVC	81
Debugging mLACP on AToM Pseudowires	81
Debugging Cross-Connect Redundancy Manager and Session Setup	82
Debugging VFI	83

Debugging the Segment Switching Manager (Switching Setup)	83
Debugging High Availability Features in mLACP	84
Configuration Examples for mLACP	85
Example Configuring VPWS	85
Active PoA for VPWS	86
Standby PoA for VPWS	86
Example Configuring VPLS	87
Active PoA for VPLS	87
Standby PoA for VPLS	88
Example Configuring H-VPLS	89
Active PoA for H-VPLS	89
Standby PoA for H-VPLS	90
Example Verifying VPWS on an Active PoA	91
show lacp multichassis group	91
show lacp multichassis port-channel	91
show mpls ldp iccp	92
show mpls l2transport	92
show etherchannel summary	92
show etherchannel number port-channel	93
show lacp internal	93
Example Verifying VPWS on a Standby PoA	93
show lacp multichassis group	94
show lacp multichassis portchannel	94
show mpls ldp iccp	95
show mpls l2transport	95
show etherchannel summary	95
show lacp internal	95
Example Verifying VPLS on an Active PoA	96
show lacp multichassis group	96
show lacp multichassis port-channel	96
show mpls ldp iccp	97
show mpls l2transport	97
show etherchannel summary	97
show lacp internal	98
Example Verifying VPLS on a Standby PoA	98

show lacp multichassis group	98
show lacp multichassis portchannel	99
show mpls ldp iccp	99
show mpls l2transport vc 2	100
show etherchannelsummary	100
show lacp internal	100
Glossary	101



CHAPTER 1

ITU-T G.8032 Ethernet Ring Protection Switching

The ITU-T G.8032 Ethernet Ring Protection Switching feature implements protection switching mechanisms for Ethernet layer ring topologies. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

- [Prerequisites for Configuring ITU-T G.8032 Ethernet Ring Protection Switching, page 1](#)
- [About ITU-T G.8032 Ethernet Ring Protection Switching, page 1](#)
- [How to Configure ITU-T G.8032 Ethernet Ring Protection Switching, page 8](#)
- [Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching, page 20](#)

Prerequisites for Configuring ITU-T G.8032 Ethernet Ring Protection Switching

- The Ethernet Flow Points (EFPs) must be configured.

About ITU-T G.8032 Ethernet Ring Protection Switching

Ring Protection Links

An Ethernet ring consists of multiple Ethernet ring nodes. Each Ethernet ring node is connected to adjacent Ethernet ring nodes using two independent ring links. A ring link prohibits formation of loops that affect the network. The Ethernet ring uses a specific link to protect the entire Ethernet ring. This specific link is called the Ring Protection Link (RPL). A ring link is bound by two adjacent Ethernet ring nodes and a port for a ring link (also known as a ring port). There must be at least two Ethernet ring nodes in a Ethernet ring.

ITU-T G.8032 Ethernet Ring Protection Switching Functionality

The Ethernet ring protection functionality includes the following:

- Loop avoidance
- The use of learning, forwarding, and Filtering Database (FDB) mechanisms

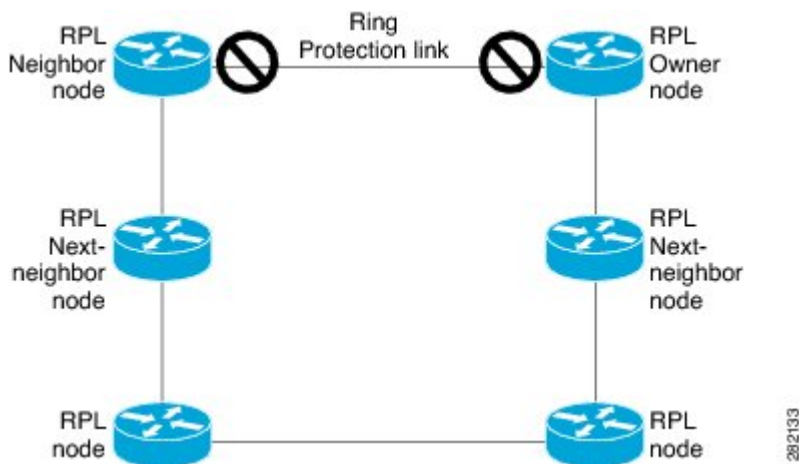
Loop avoidance in an Ethernet ring is achieved by ensuring that, at any time, traffic flows on all but the Ring Protection Link (RPL).

The following is a list of RPL types (or RPL nodes) and their functions:

- RPL owner—Responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic. There can be only one RPL owner in a ring.
- RPL neighbor node—An Ethernet ring node adjacent to the RPL. It is responsible for blocking its end of the RPL under normal conditions. This node type is optional and prevents RPL usage when protected.
- RPL next-neighbor node—Next-neighbor node is an Ethernet ring node adjacent to an RPL owner node or RPL neighbor node. It is mainly used for FDB flush optimization on the ring. This node is also optional.

The following figure illustrates the G.8032 Ethernet ring topology.

Figure 1: G.8032 Ethernet Ring Topology



R-APS Control Messages

Nodes on the ring use control messages called Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the ring protection link (RPL) on and off. Any failure along the ring triggers a R-APS Signal Failure (R-APS SF) message in both directions of the nodes adjacent to the failed link, after the nodes have blocked the port facing the failed link. On obtaining this message, the RPL owner unblocks the RPL port.

**Note**

A single link failure in the ring ensures a loop-free topology.

CFM Protocols and Link Failures

Connectivity Fault Management (CFM) and line status messages are used to detect ring link and node failure. During the recovery phase, when the failed link is restored, the nodes adjacent to the restored link send Ring Automatic Protection Switching (R-APS) No Request (R-APS NR) messages. On obtaining this message, the ring protection link (RPL) owner blocks the RPL port and sends R-APS NR and R-APS RPL (R-APS NR, RB) messages. These messages cause all other nodes, other than the RPL owner in the ring, to unblock all blocked ports. The Ethernet Ring Protection (ERP) protocol works for both unidirectional failure and multiple link failure scenarios in a ring topology.

**Note**

The G.8032 Ethernet Ring Protection (ERP) protocol uses CFM Continuity Check Messages (CCMs) at an interval of 3.3 milliseconds (ms). At this interval (which is supported only on selected platforms), SONET-like switching time performance and loop-free traffic can be achieved.

G.8032 Ring-Supported Commands and Functionality

A G.8032 ring supports these basic operator administrative commands:

- Force switch (FS)—Allows the operator to forcefully block a particular ring port. Note the following points about FS commands:
 - Effective even if there is an existing SF condition
 - Multiple FS commands for ring are supported
 - May be used to allow immediate maintenance operations
- Manual switch (MS)—Allows the operator to manually block a particular ring port. Note the following points about MS commands:
 - Ineffective in an existing FS or signal failure (SF) condition
 - Overridden by new FS or SF conditions
 - Multiple MS commands cancel all MS commands
- Clear—Cancels an existing FS or MS command on the ring port. The Clear command is used at the ring protection link (RPL) owner to clear a nonrevertive mode condition.

A G.8032 ring can support multiple instances. An instance is a logical ring running over a physical ring. Such instances are used for various reasons, such as load-balancing VLANs over a ring. For example, odd-numbered VLANs may go in one direction of the ring, and even-numbered VLANs may go in the other direction. Specific VLANs can be configured under only one instance. They cannot overlap multiple instances. Otherwise, data traffic or Ring Automatic Protection Switching (R-APS) messages may cross logical rings, which is not desirable.

G.8032 ERP Timers

The G.8032 Ethernet Ring Protection (ERP) protocol specifies the use of different timers to avoid race conditions and unnecessary switching operations:

- Delay timers—Used by the Ring Protection Link (RPL) owner to verify that the network has stabilized before blocking the RPL. Note the following points about delay timers.
 - After a signal failure (SF) condition, a Wait-to-Restore (WTR) timer is used to verify that the SF is not intermittent.
 - The WTR timer can be configured by the operator. The default time interval is 5 minutes; the time interval ranges from 1 to 12 minutes.
 - After a force switch (FS) or a manual switch (MS) command is issued, a Wait-to-Block (WTB) timer is used to verify that no background condition exists.

**Note**

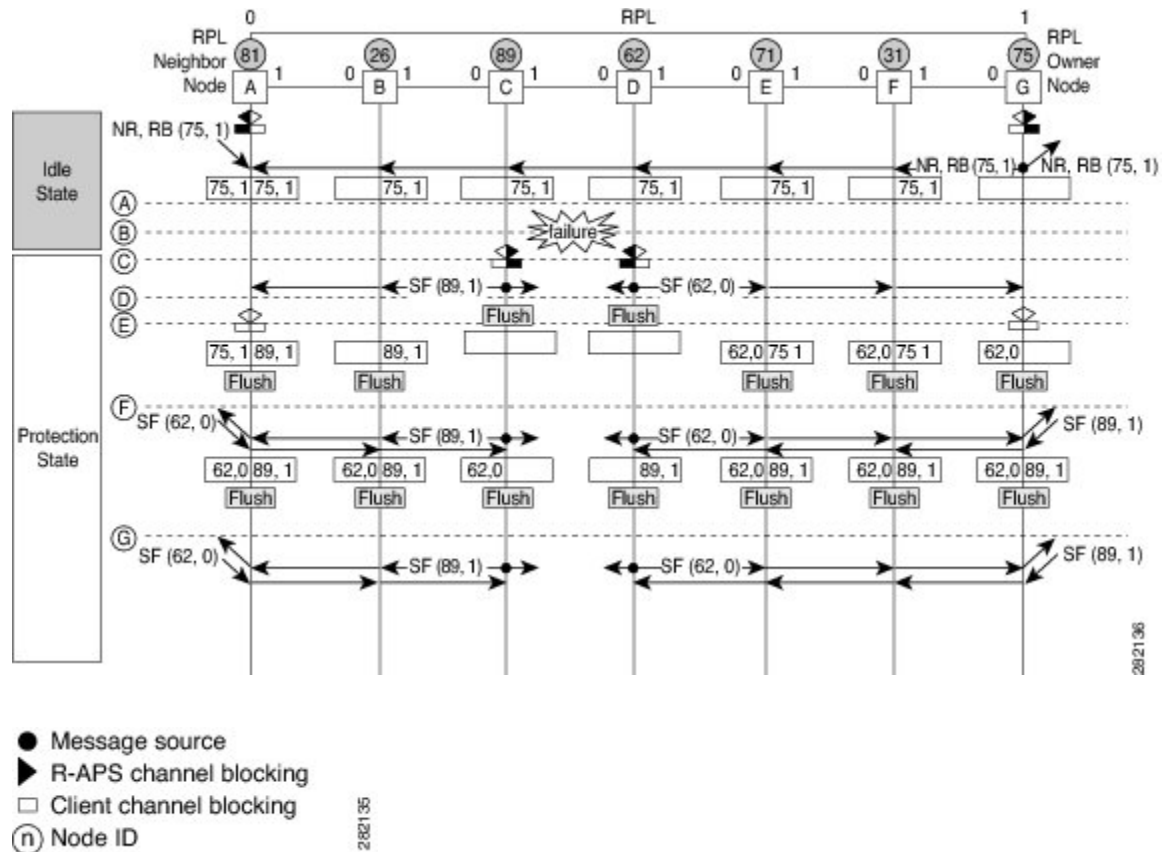
The WTB timer interval may be shorter than the WTR timer interval.

- Guard timer—Used by all nodes when changing state; the guard timer blocks latent outdated messages from causing unnecessary state changes. The guard timer can be configured. The default time interval is 500 ms; the time interval ranges from 10 to 2000 ms.
- Hold-off timers—Used by the underlying Ethernet layer to filter out intermittent link faults. The hold-off timer can be configured. The default time interval is 0 seconds; the time interval ranges from 0 to 10 seconds. Faults are reported to the ring protection mechanism only if this timer expires.

Protection Switching Functionality in a Single Link Failure and Recovery

The following figure illustrates protection switching functionality in a single-link failure.

Figure 2: G.8032 Ethernet Ring Protection Switching in a Single-Link Failure



The figure represents an Ethernet ring topology consisting of seven Ethernet ring nodes. The ring protection link (RPL) is the ring link between Ethernet ring nodes A and G. In this topology, both ends of the RPL are blocked. Ethernet ring node G is the RPL owner node, and Ethernet ring node A is the RPL neighbor node.

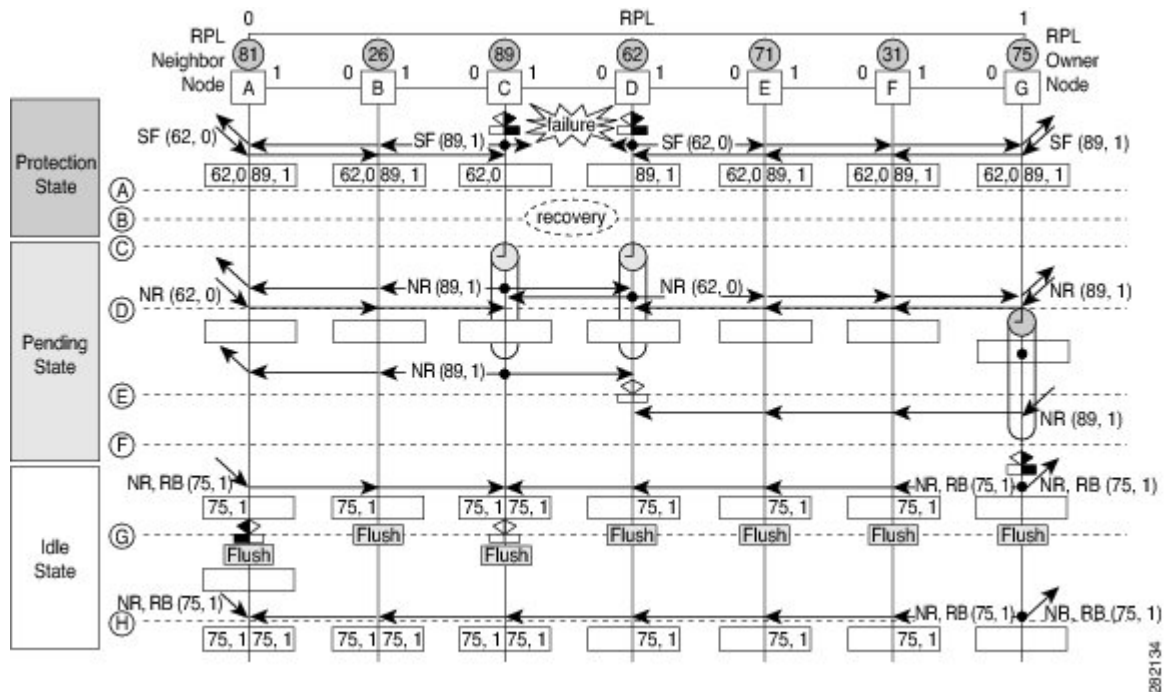
The following sequence describes the steps followed in the single-link failure:

- 1 A link operates in the normal condition.
- 2 A failure occurs.
- 3 Ethernet ring nodes C and D detect a local signal failure (SF) condition and after the hold-off time interval, block the failed ring port and perform the FDB flush.
- 4 Ethernet ring nodes C and D start sending Ring Automatic Protection Switching (R-APS) SF messages periodically along with the (node ID and bidirectional path-protected ring (BPR) identifier pair) on both ring ports while the SF condition persists.

- 5 All Ethernet ring nodes receiving an R-APS SF message perform the FDB flush. When the RPL owner node G and RPL neighbor node A receive an R-APS SF message, the Ethernet ring node unblocks its end of the RPL and performs the FDB flush.
- 6 All Ethernet ring nodes receiving a second R-APS SF message perform the FDB flush again; the additional FDB flush is because of the node ID and BPR-based configuration.
- 7 R-APS SF messages are detected on the Ethernet Ring indicating a stable SF condition. Further R-APS SF messages trigger no further action.

The following figure illustrates the steps taken in a revertive operation in a single-link failure.

Figure 3: Single-Link Failure Recovery (Revertive Operation)



The following sequence describes the steps followed in the single-link failure revertive (recovery) operation:

- 1 A link operates in the stable SF condition.
- 2 Recovery of link failure occurs.
- 3 Ethernet ring nodes C and D detect clearing of the SF condition, start the guard timer, and initiate periodic transmission of the R-APS No Request (NR) messages on both ring ports. (The guard timer prevents the reception of R-APS messages.)
- 4 When the Ethernet ring nodes receive an R-APS NR message, the node ID and BPR identifier pair of a receiving ring port is deleted and the RPL owner node starts the Wait-to-Restore (WTR) timer.
- 5 When the guard timer expires on Ethernet ring nodes C and D, the nodes may accept the new R-APS messages, if any. Ethernet ring node D receives an R-APS NR message with a higher node ID from Ethernet ring node C, and unblocks its nonfailed ring port.

- 6 When the WTR timer expires, the RPL owner node blocks its end of the RPL, sends R-APS (NR or route blocked [RB]) message with the (node ID and BPR identifier pair), and performs the FDB flush.
- 7 When Ethernet ring node C receives an R-APS (NR or RB) message, the node removes the block on its blocked ring ports, and stops sending R-APS NR messages. On the other hand, when the RPL neighbor node A receives an R-APS NR or RB message, the node blocks its end of the RPL. In addition, Ethernet ring nodes A to F perform the FDB flush when receiving an RAPS NR or RB message because of the node ID and BPR-based configuration.

Ethernet Flow Points

An Ethernet flow point (EFP) is a forwarding decision point in the provider edge (PE) router, which gives network designers flexibility to make many Layer 2 flow decisions within the interface. Many EFPs can be configured on a single physical port. (The number varies from one device to another.) EFPs are the logical demarcation points of an Ethernet virtual connection (EVC) on an interface. An EVC that uses two or more user network interfaces (UNIs) requires an EFP on the associated ingress and egress interfaces of every device that the EVC passes through.

EFPs can be configured on any Layer 2 traffic port; however, they are usually configured on UNI ports. The following parameters (matching criteria) can be configured on the EFP:

- Frames of a specific VLAN, a VLAN range, or a list of VLANs (100-150 or 100,103,110)
- Frames with no tags (untagged)
- Frames with identical double-tags (VLAN tags) as specified
- Frames with identical Class of Service (CoS) values

A frame passes each configured match criterion until the correct matching point is found. If a frame does not fit any of the matching criteria, it is dropped. Default criteria can be configured to avoid dropping frames.

The following types of commands can be used in an EFP:

- Rewrite commands—In each EFP, VLAN tag management can be specified with the following actions:
 - Pop—1) pops out a tag; 2) pops out two tags
 - Push—1) pushes in a tag; 2) pushes in two tags
 - Translate—1 to 1) changes a tag value; 1 to 2) pops one tag and pushes two tags; 2 to 1) pops two tags and pushes one tag; 2 to 2) changes the value for two tags
- Forwarding commands—Each EFP specifies the forwarding command for the frames that enter the EFP. Only one forwarding command can be configured per EFP. The forwarding options are as follows:
 - Layer 2 point-to-point forwarding to a pseudowire tunnel
 - Multipoint bridge forwarding to a bridge domain entity
 - Local switch-to-switch forwarding between two different interfaces
- Feature commands—In each EFP, the QoS features or parameters can be changed and the ACL can be updated.

Service Instances and Associated EFPs

Configuring a service instance on a Layer 2 port creates a pseudoport or EFP on which you configure EVC features. Each service instance has a unique number per interface, but you can use the same number on different interfaces because service instances on different ports are not related.

An EFP classifies frames from the same physical port to one of the multiple service instances associated with that port, based on user-defined criteria. Each EFP can be associated with different forwarding actions and behavior.

When an EFP is created, the initial state is UP. The state changes to DOWN under the following circumstances:

- The EFP is explicitly shut down by a user.
- The main interface to which the EFP is associated is down or removed.
- If the EFP belongs to a bridge domain, the bridge domain is down.
- The EFP is forced down as an error-prevention measure of certain features.

Use the **service instance ethernet** interface configuration command to create an EFP on a Layer 2 interface and to enter service instance configuration mode. Service instance configuration mode is used to configure all management and control data plane attributes and parameters that apply to the service instance on a per-interface basis. The service instance number is the EFP identifier.

After the device enters service instance configuration mode, you can configure these options:

- **default**--Sets a command to its defaults
- **description**--Adds a service instance-specific description
- **encapsulation**--Configures Ethernet frame match criteria
- **exit**--Exits from service instance configuration mode
- **no**--Negates a command or sets its defaults
- **shutdown**--Takes the service instance out of service

How to Configure ITU-T G.8032 Ethernet Ring Protection Switching

Configuring the Ethernet Ring Profile

To configure the Ethernet ring profile, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032 profile** *profile-name*
4. **timer** {*guard seconds* | *hold-off seconds* | *wtr minutes*}
5. **non-revertive**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ethernet ring g8032 profile <i>profile-name</i> Example: Device(config)# ethernet ring g8032 profile profile1	Creates the Ethernet ring profile and enters Ethernet ring profile configuration mode.
Step 4	timer { <i>guard seconds</i> <i>hold-off seconds</i> <i>wtr minutes</i> } Example: Device(config-erp-profile)# timer hold-off 5	Specifies the time interval for the guard, hold-off, and Wait-to-Restore (WTR) timers.
Step 5	non-revertive Example: Device(config-erp-profile)# non-revertive	Specifies a nonrevertive Ethernet ring instance. <ul style="list-style-type: none"> • By default, Ethernet ring instances are revertive.
Step 6	end Example: Device(config-erp-profile)# end	Returns to user EXEC mode.

Configuring Ethernet CFM MEPs

Configuring Ethernet Connectivity Fault Management (CFM) maintenance endpoints (MEPs) is optional although recommended for fast failure detection and CFM monitoring. When CFM monitoring is configured, note the following points:

- Static remote MEP (RMEP) checking should be enabled.
- The MEPs should be configured to enable Ethernet fault detection.

For information about configuring Ethernet Connectivity Fault Management (CFM) maintenance endpoints (MEPs), see the “Configuring Ethernet Connectivity Fault Management in a Service Provider Network” module of the *Carrier Ethernet Configuration Guide*.

Enabling Ethernet Fault Detection for a Service

To enable Ethernet Fault Detection (EFD) for a service to achieve fast convergence, complete the following steps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm global**
4. **link-protection enable**
5. **link-protection group management vlan *vlan-id***
6. **link-protection group *group-number* pccm vlan *vlan-id***
7. **ethernet cfm domain *domain-name* level *level-id* [direction outward]**
8. **service {*ma-name* | *ma-num* | vlan-id *vlan-id* | vpn-id *vpn-id*} [port | vlan *vlan-id* [direction down]]**
9. **continuity-check [interval *time* | loss-threshold *threshold* | static rmp]**
10. **efd notify g8032**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ethernet cfm global Example: Device(config)# ethernet cfm global	Enables Ethernet CFM globally.
Step 4	link-protection enable Example: Device(config)# link-protection enable	Enables link protection globally on the router.
Step 5	link-protection group management vlan <i>vlan-id</i> Example: Device(config)# link-protection group management vlan 51	Defines the management VLAN used for link protection.
Step 6	link-protection group <i>group-number</i> pccm vlan <i>vlan-id</i> Example: Device(config)# link-protection group 2 pccm vlan 16	Specifies an ODU-to-ODU continuity check message (P-CCM) VLAN.
Step 7	ethernet cfm domain <i>domain-name</i> level <i>level-id</i> [direction outward] Example: Device(config)# ethernet cfm domain G8032 level 4	Configures the CFM domain for ODU 1 and enters Ethernet CFM configuration mode.
Step 8	service {<i>ma-name</i> <i>ma-num</i> vlan-id <i>vlan-id</i> vpn-id <i>vpn-id</i>} [port vlan <i>vlan-id</i> [direction down]] Example: Device(config-ecfm)# service 8032_service evc 8032-evc vlan 1001 direction down	Defines a maintenance association for ODU 1 and enters Ethernet CFM service instance configuration mode.

	Command or Action	Purpose
Step 9	continuity-check [<i>interval time</i> <i>loss-threshold threshold</i> <i>static rmep</i>] Example: Device(config-ecfm-srv)# continuity-check interval 3.3ms	Enables the transmission of continuity check messages (CCMs).
Step 10	efd notify g8032 Example: Device(config-ecfm-srv)# efd notify g8032	Enables CFM to notify registered protocols when a defect is detected or cleared, which matches the current fault alarm priority.
Step 11	end Example: Device(config-ecfm-srv)# end	Returns to user EXEC mode.

Configuring the Ethernet Protection Ring

To configure the Ethernet Protection Ring (EPR), complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet ring g8032** *ring-name*
4. **port0 interface** *type number*
5. **monitor service instance** *instance-id*
6. **exit**
7. **port1 {interfacetype number | none}**
8. **monitor service instance** *instance-id*
9. **exit**
10. **exclusion-list vlan-ids** *vlan-id*
11. **open-ring**
12. **instance** *instance-id*
13. **description** *descriptive-name*
14. **profile** *profile-name*
15. **rpl {port0 | port1} {owner | neighbor | next-neighbor }**
16. **inclusion-list vlan-ids** *vlan-id*
17. **aps-channel**
18. **level** *level-value*
19. **port0 service instance** *instance-id*
20. **port1 service instance** *{instance-id | none }*
21. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ethernet ring g8032 <i>ring-name</i> Example: Device(config)# ethernet ring g8032 ring1	Specifies the Ethernet ring and enters Ethernet ring port configuration mode.

	Command or Action	Purpose
Step 4	port0 interface <i>type number</i> Example: <pre>Device(config-erp-ring)# port0 interface fastethernet 0/1/0</pre>	Connects port0 of the local node of the interface to the Ethernet ring and enters Ethernet ring protection mode.
Step 5	monitor service instance <i>instance-id</i> Example: <pre>Device(config-erp-ring-port)# monitor service instance 1</pre>	Assigns the Ethernet service instance to monitor the ring port (port0) and detect ring failures.
Step 6	exit Example: <pre>Device(config-erp-ring-port)# exit</pre>	Exits Ethernet ring port configuration mode.
Step 7	port1 { <i>interfacetype number</i> none } Example: <pre>Device(config-erp-ring)# port1 interface fastethernet 0/1/1</pre>	Connects port1 of the local node of the interface to the Ethernet ring and enters Ethernet ring protection mode.
Step 8	monitor service instance <i>instance-id</i> Example: <pre>Device(config-erp-ring-port)# monitor service instance 2</pre>	Assigns the Ethernet service instance to monitor the ring port (port1) and detect ring failures. <ul style="list-style-type: none"> • The interface (to which port1 is attached) must be a subinterface of the main interface.
Step 9	exit Example: <pre>Device(config-erp-ring-port)# exit</pre>	Exits Ethernet ring port configuration mode.
Step 10	exclusion-list vlan-ids <i>vlan-id</i> Example: <pre>Device(config-erp-ring)# exclusion-list vlan-ids 2</pre>	Specifies VLANs that are unprotected by the Ethernet ring protection mechanism.
Step 11	open-ring Example: <pre>Device(config-erp-ring)# open-ring</pre>	Specifies the Ethernet ring as an open ring.

	Command or Action	Purpose
Step 12	instance <i>instance-id</i> Example: Device(config-erp-ring)# instance 1	Configures the Ethernet ring instance and enters Ethernet ring instance configuration mode.
Step 13	description <i>descriptive-name</i> Example: Device(config-erp-inst)# description cisco_customer_instance	Specifies a descriptive name for the Ethernet ring instance.
Step 14	profile <i>profile-name</i> Example: Device(config-erp-inst)# profile profile1	Specifies the profile associated with the Ethernet ring instance.
Step 15	rpl {port0 port1} {owner neighbor next-neighbor} } Example: Device(config-erp-inst)# rpl port0 neighbor	Specifies the Ethernet ring port on the local node as the RPL owner, neighbor, or next neighbor.
Step 16	inclusion-list vlan-ids <i>vlan-id</i> Example: Device(config-erp-inst)# inclusion-list vlan-ids 11	Specifies VLANs that are protected by the Ethernet ring protection mechanism.
Step 17	aps-channel Example: Device(config-erp-inst)# aps-channel	Enters Ethernet ring instance aps-channel configuration mode.
Step 18	level <i>level-value</i> Example: Device(config-erp-inst-aps)# level 5	Specifies the Automatic Protection Switching (APS) message level for the node on the Ethernet ring. <ul style="list-style-type: none"> • All nodes in the Ethernet ring must be configured with the same level.
Step 19	port0 service instance <i>instance-id</i> Example: Device(config-erp-inst-aps)# port0 service instance 100	Associates APS channel information with port0.

	Command or Action	Purpose
Step 20	port1 service instance {instance-id none } Example: Device(config-erp-inst-aps)# port1 service instance 100	Associates APS channel information with port1.
Step 21	end Example: Device(config-erp-inst-aps)# end	Returns to user EXEC mode.

Configuring Topology Change Notification Propagation

To configure topology change notification (TCN) propagation, complete the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. ethernet tcn-propagation G8032 to {REP | G8032}
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ethernet tcn-propagation G8032 to {REP G8032} Example: Device(config)# ethernet tcn-propagation G8032 to G8032	Allows topology change notification (TCN) propagation from a source protocol to a destination protocol. <ul style="list-style-type: none"> • Source and destination protocols vary by platform and release.

	Command or Action	Purpose
Step 4	end Example: Device(config)# end	Returns to user EXEC mode.

Configuring a Service Instance

To configure a service instance, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *instance-id* **ethernet** [*evc-id*]
5. **encapsulation dot1q** *vlan-id* [**native**]
6. **bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface fastethernet 4/0/0	Specifies the interface type and number.

	Command or Action	Purpose
Step 4	service instance <i>instance-id</i> ethernet [<i>evc-id</i>] Example: Device(config-if)# service instance 101 ethernet	Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.
Step 5	encapsulation dot1q <i>vlan-id</i> [native] Example: Device(config-if-srv)# encapsulation dot1q 13	Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	bridge-domain <i>bridge-id</i> [split-horizon [group <i>group-id</i>]] Example: Device(config-if-srv)# bridge-domain 12	Binds the service instance to a bridge domain instance.
Step 7	end Example: Device(config-if-srv)# end	Exits service instance configuration mode.

Verifying the Ethernet Ring Protection (ERP) Switching Configuration

To verify the ERP switching configuration, use one or more of the following commands in any order.

SUMMARY STEPS

1. **enable**
2. **show ethernet ring g8032 status** [*ring-name*] [**instance** [*instance-id*]]
3. **show ethernet ring g8032 brief** [*ring-name*] [**instance** [*instance-id*]]
4. **show ethernet ring g8032 summary**
5. **show ethernet ring g8032 statistics** [*ring-name*] [**instance** [*instance-id*]]
6. **show ethernet ring g8032 profile** [*profile-name*]
7. **show ethernet ring g8032 port status interface** [*type number*]
8. **show ethernet ring g8032 configuration** [*ring-name*] **instance** [*instance-id*]
9. **show ethernet ring g8032 trace** {ctrl [*ring-name* **instance** *instance-id*] | **sm**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ethernet ring g8032 status [<i>ring-name</i>] [<i>instance</i> [<i>instance-id</i>]] Example: Device# show ethernet ring g8032 status RingA instance 1	Displays a status summary for the ERP instance.
Step 3	show ethernet ring g8032 brief [<i>ring-name</i>] [<i>instance</i> [<i>instance-id</i>]] Example: Device# show ethernet ring g8032 brief	Displays a brief description of the functional state of the ERP instance.
Step 4	show ethernet ring g8032 summary Example: Device# show ethernet ring g8032 summary	Displays a summary of the number of ERP instances in each state of the ERP switching process.
Step 5	show ethernet ring g8032 statistics [<i>ring-name</i>] [<i>instance</i> [<i>instance-id</i>]] Example: Device# show ethernet ring g8032 statistics RingA instance 1	Displays the number of events and Ring Automatic Protection Switching (R-APS) messages received for an ERP instance.
Step 6	show ethernet ring g8032 profile [<i>profile-name</i>] Example: Device# show ethernet ring g8032 profile gold	Displays the settings for one or more ERP profiles.
Step 7	show ethernet ring g8032 port status interface [<i>type number</i>] Example: Device# show ethernet ring g8032 port status interface fastethernet 0/0/1	Displays Ethernet ring port status information for the interface.

	Command or Action	Purpose
Step 8	show ethernet ring g8032 configuration [<i>ring-name</i>] instance [<i>instance-id</i>] Example: Device# show ethernet ring g8032 configuration RingA instance 1	Displays the details of the ERP instance configuration manager.
Step 9	show ethernet ring g8032 trace {ctrl [<i>ring-name</i> instance <i>instance-id</i>] sm } Example: Device# show ethernet ring g8032 trace sm	Displays information about ERP traces.
Step 10	end Example: Device# end	Returns to privileged EXEC mode.

Configuration Examples for ITU-T G.8032 Ethernet Ring Protection Switching

Example: Configuring Ethernet Ring Protection Switching

The following is an example of an Ethernet Ring Protection (ERP) switching configuration:

```

ethernet ring g8032 profile profile_ABC
  timer wtr 1
  timer guard 100
  timer hold-off 1

ethernet ring g8032 major_ring_ABC
  exclusion-list vlan-ids 1000
  port0 interface FastEthernet 0/0/0
    monitor service instance 103
  port1 interface FastEthernet 0/1/0
    monitor service instance 102
  instance 1
    profile profile_ABC
    rpl port0 owner
    inclusion-list vlan-ids 100
    aps-channel
    port0 service instance 100
    port1 service instance 100
  !
interface FastEthernet 0/0/0
  no ip address
  service instance 100 ethernet

```

```

        encapsulation dot1q 100
        bridge-domain 100
    service instance 200 ethernet
        encapsulation dot1q 200
        bridge-domain 200

    !
    !
    interface FastEthernet 0/1/1
    no ip address
    service instance 100 ethernet
        encapsulation dot1q 100
        bridge-domain 100
    service instance 200 ethernet
        encapsulation dot1q 200
        bridge-domain 200

    !
    !

```

Example: Enabling Ethernet Fault Detection for a Service

```

ethernet cfm domain G8032 level 4
service 8032_service evc 8032-evc vlan 1001 direction down
    continuity-check
    continuity-check interval 3.3ms
    offload sampling 1000
    efd notify g8032
ethernet ring g8032 profile TEST
timer wtr 1
timer guard 100
ethernet ring g8032 open
open-ring
port0 interface GigabitEthernet0/1/3
    monitor service instance 1001
port1 none
instance 1
    profile TEST
    inclusion-list vlan-ids 2-500,1001
    aps-channel
    port0 service instance 1001
    port1 none
    !
!
instance 2
    profile TEST
    rpl port0 owner
    inclusion-list vlan-ids 1002,1005-2005
    aps-channel
    port0 service instance 1002
    port1 none
    !

interface GigabitEthernet0/1/3
no ip address
load-interval 30
shutdown
negotiation auto
storm-control broadcast level 10.00
storm-control multicast level 10.00
storm-control unicast level 90.00
service instance 1 ethernet
    encapsulation untagged
    l2protocol peer lldp
    bridge-domain 1
!
service instance trunk 10 ethernet
    encapsulation dot1q 2-500,1005-2005
    rewrite ingress tag pop 1 symmetric

```

```

    bridge-domain from-encapsulation
!
service instance 1001 ethernet 8032-evc
    encapsulation dot1q 1001
    rewrite ingress tag pop 1 symmetric
    bridge-domain 1001
    cfm mep domain G8032 mpid 20
!
service instance 1002 ethernet 8032-evc-1
    encapsulation dot1q 1002
    rewrite ingress tag pop 1 symmetric
    bridge-domain 1002
!
End

```

Example: Verifying the Ethernet Ring Protection Configuration

The following is sample output from the **show ethernet ring g8032 configuration** command. Use this command to verify if the configuration entered is valid and to check for any missing configuration parameters.

```

Device# show ethernet ring g8032 configuration

ethernet ring ring0
Port0: GigabitEthernet0/0/0 (Monitor: GigabitEthernet0/0/0)
Port1: GigabitEthernet0/0/4 (Monitor: GigabitEthernet0/0/4)
Exclusion-list VLAN IDs: 4001-4050
Open-ring: no
Instance 1
Description:
Profile:     opp
RPL:
Inclusion-list VLAN IDs: 2,10-500
APS channel
Level: 7
Port0: Service Instance 1
Port1: Service Instance 1
State: configuration resolved

```



Configuring IEEE 802.3ad Link Bundling

This document describes how the IEEE 802.3ad Link Bundling feature leverages the EtherChannel infrastructure within Cisco IOS XE software to manage the bundling of Ethernet links. The supported Ethernet link types for link bundling are Gigabit Ethernet and Ten Gigabit Ethernet.

- [Prerequisites for Configuring IEEE 802.3ad Link Bundling, page 23](#)
- [Restrictions for Configuring IEEE 802.3ad Link Bundling, page 23](#)
- [Information About Configuring IEEE 802.3ad Link Bundling, page 24](#)
- [How to Configure IEEE 802.3ad Link Bundling, page 29](#)
- [Configuration Examples for IEEE 802.3ad Link Bundling, page 44](#)

Prerequisites for Configuring IEEE 802.3ad Link Bundling

- Knowledge of how EtherChannels and Link Aggregation Control Protocol (LACP) function in a network
- Verification that both ends of the LACP link have the same baseline software version

Restrictions for Configuring IEEE 802.3ad Link Bundling

- The maximum number of Ethernet links per bundle that can be supported varies by platform. Some platforms support 4 while other platforms support a maximum a 16.
- All links must operate at the same link speed and in full-duplex mode (LACP does not support half-duplex mode).
- All links must be configured as either EtherChannel links or LACP links.
- Only physical interfaces can form aggregations. Aggregations of VLAN interfaces are not possible nor is an aggregation of aggregations.
- If a router is connected to a switch, the bundle terminates on the switch.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.

- All ports in an EtherChannel must use the same EtherChannel protocol.
- Maximum of four bundled ports per Ethernet port channel are supported.
- The maximum number of bundled ports per Ethernet port channel that can be supported varies by platform. Some platforms support 4 while other platforms support 16.
- Maximum of 64 Ethernet port channels in a chassis are supported.
- Quality of service (QoS) is supported on individual bundled ports and not on Ethernet port channels.

Information About Configuring IEEE 802.3ad Link Bundling

Gigabit EtherChannel

Gigabit EtherChannel (GEC) is high-performance Ethernet technology that provides Gigabit per second (Gb/s) transmission rates. A Gigabit EtherChannel bundles individual Ethernet links (Gigabit Ethernet or Ten Gigabit Ethernet) into a single logical link that provides the aggregate bandwidth of up to four physical links. All LAN ports in each EtherChannel must be the same speed and all must be configured as either Layer 2 or Layer 3 LAN ports. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link in the EtherChannel.

When a link within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining links within that EtherChannel. Also when a failure occurs, a trap is sent that identifies the device, the EtherChannel, and the failed link.

Port-Channel and LACP-Enabled Interfaces

Each EtherChannel has a numbered port-channel interface that must be manually created before interfaces can be added to the channel group. The configuration of a port-channel interface affects all LAN ports assigned to that port-channel interface.

To change the parameters of all ports in an EtherChannel, change the configuration of the port-channel interface; for example, if you want to configure Spanning Tree Protocol or configure a Layer 2 EtherChannel as a trunk. Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port-channel; that is, configuration changes are propagated to the physical interfaces that are not part of the port-channel but are part of the channel group.

The configuration of a LAN port affects only that LAN port.

IEEE 802.3ad Link Bundling

The IEEE 802.3ad Link Bundling feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. This feature helps improve the cost effectiveness of a device by increasing cumulative bandwidth without necessarily requiring hardware upgrades. In addition, IEEE 802.3ad Link Bundling provides a capability to dynamically provision, manage, and monitor various aggregated links and enables interoperability between various Cisco devices and devices of third-party vendors.

LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in passive and active modes. The protocol “learns” the

capabilities of LAN port groups dynamically and informs the other LAN ports. After LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. Then the EtherChannel is added to the spanning tree as a single bridge port.

Both the passive and active modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. (Layer 2 EtherChannels also use VLAN numbers.) LAN ports can form an EtherChannel when they are in compatible LACP modes, as in the following examples:

- A LAN port in active mode can form an EtherChannel with another LAN port that is in active mode.
- A LAN port in active mode can form an EtherChannel with another LAN port in passive mode.
- A LAN port in passive mode cannot form an EtherChannel with another LAN port that is also in passive mode because neither port will initiate negotiation.

LACP uses the following parameters:

- LACP system priority—You must configure an LACP system priority on each device running LACP. The system priority can be configured automatically or through the command-line interface (CLI). LACP uses the system priority with the device MAC address to form the system ID and also during negotiation with other systems.
- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. LACP also uses the port priority with the port number to form the port identifier.
- LACP administrative key—LACP automatically configures an administrative key value on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the following:
 - Port physical characteristics such as data rate, duplex capability, and point-to-point or shared medium
 - Configuration restrictions that you establish

On ports configured to use LACP, it tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware. To use the hot standby feature in the event a channel port fails, both ends of the LACP bundle must support the **lacp max-bundle** command.

As a control protocol, LACP uses the Slow Protocol Multicast address of 01-80-C2-00-00-02 to transmit LACP protocol data units (PDUs). Aside from LACP, the Slow Protocol linktype is to be utilized by operations, administration, and maintenance (OAM) packets, too. Subsequently, a subtype field is defined per the IEEE 802.3ad standard [1] (Annex 43B, section 4) differentiating LACP PDUs from OAM PDUs.

**Note**

LACP and Port Aggregation Control Protocol (PAgP) are not compatible. Ports configured for PAgP cannot form port channels on ports configured for LACP, and ports configured for LACP cannot form port channels on ports configured for PAgP.

Benefits of IEEE 802.3ad Link Bundling

- Increased network capacity without changing physical connections or upgrading hardware
- Cost savings from the use of existing hardware and software for additional functions
- A standard solution that enables interoperability of network devices
- Port redundancy without user intervention when an operational port fails

LACP Enhancements

The following LACP enhancements are supported:

- Four member links per LACP bundle.
- Stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles.
- Link failover time of 250 milliseconds or less and a maximum link failover time of 2 seconds; port channels remain in the LINK_UP state to eliminate reconvergence by the Spanning-Tree Protocol.
- Shutting down a port channel when the number of active links falls below the minimum threshold. In the port channel interface, a configurable option is provided to bring down the port channel interface when the number of active links falls below the minimum threshold. For the port-channel state to be symmetric on both sides of the channel, the peer must also be running LACP and have the same **lacp min-bundle** command setting.
- The IEEE Link Aggregation Group (LAG) MIB.

LACP for Gigabit Interfaces

The LACP (802.3ad) for Gigabit Interfaces feature bundles individual Ethernet links (Gigabit Ethernet or Ten Gigabit Ethernet) into a single logical link that provides the aggregate bandwidth of up to four physical links.

All LAN ports on a port channel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports. If a segment within a port channel fails, traffic previously carried over the failed link switches to the remaining segments within the port channel. Inbound broadcast and multicast packets on one segment in a port channel are blocked from returning on any other segment of the port channel.



Note

The network device may impose its own limits on the number of bundled ports per port channel.

Features Supported on Gigabit EtherChannel Bundles

The table below lists the features that are supported on Gigabit EtherChannel (GEC) bundles.

Table 1: Gigabit EtherChannel Bundle Features

Cisco IOS XE Release	Feature	Bundle Interface
2.5	Access control lists (ACLs) per bundle	Supported
	All Ethernet routing protocols	Supported
	Intelligent Service Gateway (ISG) IP sessions	Not Supported
	Interface statistics	Supported
	IP switching	Supported
	IPv4: unicast and multicast	Supported
	IPv6: unicast without load balancing across member links	Supported
	IPv6: multicast	Not Supported
	Layer 2 Tunneling Protocol Version 3 (L2TPv3), Generic Routing Encapsulation (GRE), IPinIP, Any Transport Over Multiprotocol Label Switching (MPLS) (AToM) tunnels	Supported
	Layer 2 Tunneling Protocol Version 2 (L2TPv2)	Not Supported
	MPLS (6PE)	Supported
	Multicast VPN	Not Supported
	VLANs	Supported
2.6	Virtual Private Network (VPN) Routing and Forwarding (VRF)	Supported
3.4	IPv6: unicast and multicast	Supported
3.6	Bidirectional Forwarding Detection (BFD) over GEC	Supported
3.7	Layer 2 Tunneling Protocol Version 2 (L2TPv2)	Supported

Cisco IOS XE Release	Feature	Bundle Interface
	PPPoX (PPPoEoE, PPPoEoQinQ, PPPoVLAN)	Supported
3.7.6	Policy-based routing (PBR) over GEC	Supported
3.11	GEC over L2TPv3	Supported
3.12	MPLS TE (Traffic Engineering) over GEC	Supported

Guidelines for LACP for Gigabit Interfaces Configuration

Port channel interfaces that are configured improperly with LACP are disabled automatically to avoid network loops and other problems. To avoid configuration problems, observe these guidelines and restrictions:

- Every port added to a port channel must be configured identically. No individual differences in configuration are allowed.
- Bundled ports can be configured on different line cards in a chassis.
- Maximum transmission units (MTUs) must be configured on only port channel interfaces; MTUs are propagated to the bundled ports.
- QoS and committed access rate (CAR) are applied at the port level. Access control lists (ACLs) are applied on port channels.
- MAC configuration is allowed only on port channels.
- MPLS IP should be enabled on bundled ports using the **mpls ip** command.
- Unicast Reverse Path Forwarding (uRPF) should be applied on the port channel interface using the **ip verify unicast reverse-path** command in interface configuration mode.
- Cisco Discovery Protocol should be enabled on the port channel interface using the **cdp enable** command in interface configuration mode.
- All LAN ports in a port channel should be enabled. If you shut down a LAN port in a port channel, the shutdown is treated as a link failure and the traffic is transferred to one of the remaining ports in the port channel.
- Create a port channel interface using the **interface port-channel** command in global configuration mode.
- When an Ethernet interface has an IP address assigned, disable that IP address before adding the interface to the port channel. To disable an existing IP address, use the **no ip address** command in interface configuration mode.
- The **hold queue in** command is valid only on port channel interfaces. The **hold queue out** command is valid only on bundled ports.

How to Configure IEEE 802.3ad Link Bundling

Enabling LACP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel *channel-number***
4. **channel-group *channel-group-number* mode {active | passive}**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface port-channel <i>channel-number</i> Example: Device(config)# interface port-channel 10	Identifies the interface port channel and enters interface configuration mode.
Step 4	channel-group <i>channel-group-number</i> mode {active passive} Example: Device(config-if)# channel-group 25 mode active	Configures the interface in a channel group and sets it as active. In active mode, the port will initiate negotiations with other ports by sending LACP packets.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Configuring a Port Channel

You must manually create a port channel logical interface. Perform this task to configure a port channel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-number*
4. **lacp max-bundle** *max-bundles*
5. **ip address** *ip-address mask*
6. **end**
7. **show running-config interface port-channel** *group-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface port-channel <i>channel-number</i> Example: Device(config)# interface port-channel 10	Identifies the interface port channel and enters interface configuration mode.
Step 4	lacp max-bundle <i>max-bundles</i> Example: Device(config-if)# lacp max-bundle 3	Configures three active links on the port channel. The remaining links are in standby mode. Traffic is load-balanced among the active links.
Step 5	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 172.31.52.10 255.255.255.0	Assigns an IP address and subnet mask to the EtherChannel.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 7	show running-config interface port-channel <i>group-number</i> Example: Device# show running-config interface port-channel 10	Displays the port channel configuration.

Example

This example shows how to verify the configuration:

```
Device# show running-config interface port-channel 10

Building configuration...
Current configuration:
!
interface Port-channel10
 ip address 172.31.52.10 255.255.255.0
 no ip directed-broadcast
end
```

Configuring LACP (802.3ad) for Gigabit Interfaces

Perform this task to create a port channel with two bundled ports. You can configure a maximum of four bundled ports per port channel.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface port-channel *number*
4. ip address *ip-address mask*
5. interface *type slot/subslot// port*
6. no ip address
7. channel-group *channel-group-number* mode {active | passive}
8. exit
9. interface *type slot/subslot// port*
10. no ip address
11. channel-group *channel-group-number* mode {active | passive}
12. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface port-channel <i>number</i> Example: Device(config)# interface port-channel 1	Specifies the port channel interface and enters interface configuration mode. <ul style="list-style-type: none"> • <i>number</i> —Valid range is from 1 to 64.
Step 4	ip address <i>ip-address mask</i> Example: Device(config-if)# ip address 10.1.1.1 255.255.255.0	Assigns an IP address and subnet mask to the port channel interface.
Step 5	interface <i>type slot/subslot// port</i> Example: Device(config-if)# interface gigabitethernet 2/0/0	Specifies the port to bundle.
Step 6	no ip address Example: Device(config-if)# no ip address	Disables the IP address on the port channel interface.
Step 7	channel-group <i>channel-group-number</i> mode {active passive} Example: Device(config-if)# channel-group 1 mode active	Assigns the interface to a port channel group and sets the LACP mode. <ul style="list-style-type: none"> • <i>channel-group-number</i> —Valid range is 1 to 64. • active —Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets. • passive —Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the channel group attaches the interface to the bundle.

	Command or Action	Purpose
Step 8	exit Example: Device(config-if)# exit	Returns to global configuration mode.
Step 9	interface <i>type slot/subslot/port</i> Example: Device(config)# interface gigabitethernet 4/0/0	Specifies the next port to bundle and places the CLI in interface configuration mode.
Step 10	no ip address Example: Device(config-if)# no ip address	Disables the IP address on the port channel interface.
Step 11	channel-group <i>channel-group-number</i> mode { active passive } Example: Device(config-if)# channel-group 1 mode active	Assigns the interface to the previously configured port channel group. <ul style="list-style-type: none"> • <i>channel-group-number</i> —Valid range is 1 to 64. • active —Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets. • passive —Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the channel-group attaches the interface to the bundle.
Step 12	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Example

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 1
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# interface gigabitethernet 2/0/0
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# exit
Device(config)# interface gigabitethernet 4/0/0
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# end

```

Setting LACP System Priority and Port Priority

Perform this task to set the LACP system priority and port priority. The system ID is the combination of the LACP system priority and the MAC address of a device. The port identifier is the combination of the port priority and port number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lacp system-priority *priority***
4. **interface *slot/subslot/ port***
5. **lacp port-priority *priority***
6. **end**
7. **show lacp sys-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	lacp system-priority <i>priority</i> Example: Device(config)# lacp system-priority 200	Sets the system priority.
Step 4	interface <i>slot/subslot/ port</i> Example: Device(config)# interface gigabitethernet 0/1/1	Specifies the bundled port on which to set the LACP port priority and enters interface configuration mode.
Step 5	lacp port-priority <i>priority</i> Example: Device(config-if)# lacp port-priority 500	Specifies the priority for the physical interface. <ul style="list-style-type: none"> • <i>priority</i> —Valid range is from 1 to 65535. The higher the number, the lower the priority.

	Command or Action	Purpose
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show lacp sys-id Example: Device# show lacp 200	Displays the system ID (a combination of the system priority and the MAC address of the device).

Examples

```
Device> enable
Device# configure terminal
Device(config)# lacp system-priority 200
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# lacp port-priority 500
Device(config-if)# end
```

This example shows how to verify the LACP configuration:

```
Device# show lacp 200
200.abcd.abcd.abcd.
```

Adding and Removing Interfaces from a Link Bundle

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/subslot/port*
4. **channel-group** *channel-group-number* **mode** {**active** | **passive**}
5. **no channel-group** *channel-group-number* **mode** {**active** | **passive**}
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/subslot/port</i> Example: Device(config)# interface gigabitethernet 5/0/0	Configures a Gigabit Ethernet interface.
Step 4	channel-group <i>channel-group-number</i> mode { active passive } Example: Device(config-if)# channel-group 5 mode active	Adds an interface to a channel group and enters interface configuration mode. • In this instance, the interface from Step 3 is added.
Step 5	no channel-group <i>channel-group-number</i> mode { active passive } Example: Device(config-if)# no channel-group 5 mode active	Removes the Gigabit Ethernet interface from channel group.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Removing a Channel Group from a Port

Perform this task to remove a Gigabit Ethernet port channel group from a physical port.

SUMMARY STEPS

1. enable
2. configure terminal
3. no interface port-channel *number*
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	no interface port-channel <i>number</i> Example: Device(config)# no interface port-channel 1	Removes the specified port channel group from a physical port. <ul style="list-style-type: none"> <i>number</i>—Valid range is from 1 to 16.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.

Example

```
Device> enable
Device# configure terminal
Device(config)# no interface port-channel 1
Device(config)# end
```

Setting a Minimum Threshold of Active Links

SUMMARY STEPS

1. enable
2. configure terminal
3. interface *type number*
4. lacp min-bundle *min-bundle*
5. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Device(config)# interface port-channel 1	Creates a port-channel virtual interface and enters interface configuration mode.
Step 4	lacp min-bundle <i>min-bundle</i> Example: Device(config-if)# lacp min-bundle 4	Sets the minimum threshold of active links to 4.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Monitoring LACP Status

SUMMARY STEPS

1. enable
2. show lacp {*number* | counters | internal | neighbor | sys-id}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	show lacp {<i>number</i> counters internal neighbor sys-id} Example: Device# show lacp internal	Displays internal device information.

Troubleshooting Tips

To verify and isolate a fault, start at the highest level maintenance domain and do the following:

- 1 Check the device error status.
- 2 When a error exists, perform a loopback test to confirm the error.
- 3 Run a traceroute to the destination to isolate the fault.
- 4 If the fault is identified, correct the fault.
- 5 If the fault is not identified, go to the next lower maintenance domain and repeat steps 1 through 4 at that maintenance domain level.
- 6 Repeat the first four steps, as needed, to identify and correct the fault.

Displaying Gigabit EtherChannel Information

To display Gigabit Ethernet port channel information, use the **show interfaces port-channel** command in user EXEC mode or privileged EXEC mode. The following example shows information about port channels configured on ports 0/2 and 0/3. The default MTU is set to 1500 bytes.

```
Device# show interfaces port-channel 1
Port-channell is up, line protocol is up
Hardware is GEChannel, address is 0013.19b3.7748 (bia 0000.0000.0000)
MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
No. of active members in this channel: 2
Member 0 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet7/1/0 ,
Full-duplex, 1000Mb/s
Last input 00:00:05, output never, output hang never
Last clearing of "show interface" counters 00:04:40
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Interface Port-channell queueing strategy: PXF First-In-First-Out
Output queue 0/8192, 0 drops; input queue 0/75, 0 drops
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 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
3 packets output, 180 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
The table below describes the significant fields shown in the display.
```

Table 2: show interfaces port-channel Field Descriptions

Field	Description
Port-channel1 is up, line protocol is up	Indicates the bundle interface is currently active and can transmit and receive or it has been taken down by an administrator.
Hardware is	Hardware type (Gigabit EtherChannel).
address is	Address being used by the interface.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface, in kilobits per second.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
tx load rxload	Transmit and receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the bandwidth interface configuration command.
Encapsulation	Encapsulation type assigned to the interface.
loopback	Indicates if loopbacks are set.
keepalive	Indicates if keepalives are set.
ARP type	Address Resolution Protocol (ARP) type on the interface.
ARP Timeout	Number of hours, minutes, and seconds an ARP cache entry stays in the cache.
No. of active members in this channel	Number of bundled ports (members) currently active and part of the port channel group.
Member <no.> Gigabit Ethernet: <no. /no. /no. >	Number of the bundled port and associated Gigabit Ethernet port channel interface.

Field	Description
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed locally on the Device. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
output hang	Number of hours, minutes, and seconds since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates that the elapsed time is too long to be displayed. 0:00:00 indicates that the counters were cleared more than 231 ms and less than 232 ms ago.
Input queue	Number of packets in the input queue and the maximum size of the queue.
Queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in the output queue and the maximum size of the queue.
5 minute input rate 5 minute output rate	Average number of bits and packets received or transmitted per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.

Field	Description
bytes (input)	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Broadcast storms on Ethernet lines and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size for the medium.
input errors	Total number of no buffer, runts, giants, cyclic redundancy checks (CRCs), frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum might not balance with the other counts.
CRC	CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus. A high number of CRCs is usually the result of collisions or a station transmitting bad data. On a serial link, CRCs usually indicate noise, gain hits or other transmission problems on the data link.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
overrun	Number of times the serial receiver hardware was unable to pass received data to a hardware buffer because the input rate exceeded the receiver's capacity for handling the data.

Field	Description
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
watchdog	Number of times the watchdog receive timer expired.
multicast	Number of multicast packets received.
packets output	Total number of messages transmitted by the system.
bytes (output)	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the far-end transmitter has been running faster than the near-end Device's receiver can handle.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors, as some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up but the line protocol is down, the system periodically resets the interface in an effort to restart that interface. Interface resets can also occur when an unrecoverable interface processor error occurred, or when an interface is looped back or shut down.
babbles	The transmit jabber timer expired.

Field	Description
late collision	Number of late collisions. Late collision happens when a collision occurs after transmitting the preamble. The most common cause of late collisions is that your Ethernet cable segments are too long for the speed at which you are transmitting.
deferred	Indicates that the chip had to defer while ready to transmit a frame because the carrier was asserted.
lost carrier	Number of times the carrier was lost during transmission.
no carrier	Number of times the carrier was not present during the transmission.
PAUSE output	Not supported.
output buffer failures	Number of times that a packet was not output from the output hold queue because of a shortage of shared memory.
output buffers swapped out	Number of packets stored in main memory when the output queue is full; swapping buffers to main memory prevents packets from being dropped when output is congested. The number is high when traffic is bursty.

Configuration Examples for IEEE 802.3ad Link Bundling

Example: Configuring LACP for Gigabit Interfaces

The following example shows how to configure Gigabit Ethernet ports 2/0 and 4/0 into port channel 1 with LACP parameters.

```

Device> enable
Device# configure terminal
Device(config)# lacp system-priority 65535
Device(config)# interface port-channel 1
Device(config-if)# lacp max-bundle 1
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# no ip address
Device(config-if)# lacp port-priority 100
Device(config-if)# channel-group 1 mode passive
Device(config-if)# exit
Device(config)# interface gigabitethernet 4/0/0
Device(config-if)# no ip address
Device(config-if)# lacp port-priority 200

```

```
Device(config-if)# channel-group 1 mode passive
Device(config-if)# end
```

Example Associating a Channel Group with a Port Channel

This example shows how to configure channel group number 5 and include it in the channel group.

```
Device1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device1(config)# interface port 5
Device1(config-if)#
*Aug 20 17:06:14.417: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel5, changed
state to down
*Aug 20 17:06:25.413: %LINK-3-UPDOWN: Interface Port-channel5, changed state to down
Device1(config-if)#
Device1(config-if)# interface gigabitethernet 7/0/0
Device1(config-if)# channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:07:43.713: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to down
*Aug 20 17:07:44.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
changed state to down
*Aug 20 17:07:45.093: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 7/0/0 Physical Port Link
Down
*Aug 20 17:07:45.093: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 7/0/0 Physical Port Link Down

*Aug 20 17:07:47.093: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to up
*Aug 20 17:07:48.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
changed state to up
*Aug 20 17:07:48.957: GigabitEthernet7/0/0 added as member-1 to port-channel5

*Aug 20 17:07:51.957: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel5, changed
state to up
Device1(config-if)# end
Device1#
*Aug 20 17:08:00.933: %SYS-5-CONFIG_I: Configured from console by console
Device1# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
Channel group 5

Port      Flags    State    Priority    Key        Oper       Port      Port
Gi7/0/0   SA       bndl     32768      0x5        0x5        0x43      0x3D
Device1# show interface port 5
Port-channel5 is up, line protocol is up
  Hardware is GEChannel, address is 0014.a93d.4aa8 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 1
      Member 0 : GigabitEthernet7/0/0 , Full-duplex, 1000Mb/s
  Last input 00:00:05, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Interface Port-channel5 queueing strategy: PXF First-In-First-Out
  Output queue 0/8192, 0 drops; input queue 0/75, 0 drops
  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 no buffer
  Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    9 packets output, 924 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

Example Adding and Removing Interfaces from a Bundle

The following example shows how to add an interface to a bundle:

```

Device1# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
Channel group 5

Port      Flags   State   LACP port   Admin   Oper   Port   Port
Gi7/0/0   SA       bndl    32768       0x5     0x5    0x43   0x3D
Device1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device1(config)# interface gigabitethernet 5/0/0
Device1(config-if)# channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:10:19.057: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to down
*Aug 20 17:10:19.469: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 5/0/0 Physical Port Link
Down
*Aug 20 17:10:19.473: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 5/0/0 Physical Port Link Down

*Aug 20 17:10:21.473: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to up
*Aug 20 17:10:21.473: GigabitEthernet7/0/0 taken out of port-channel5
*Aug 20 17:10:23.413: GigabitEthernet5/0/0 added as member-1 to port-channel5

*Aug 20 17:10:23.473: %LINK-3-UPDOWN: Interface Port-channel5, changed state to up
Device1(config-if)# end
Device1#
*Aug 20 17:10:27.653: %SYS-5-CONFIG_I: Configured from console by console
*Aug 20 17:11:40.717: GigabitEthernet7/0/0 added as member-2 to port-channel5

Device1# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
Channel group 5

Port      Flags   State   LACP port   Admin   Oper   Port   Port
Gi7/0/0   SA       bndl    32768       0x5     0x5    0x43   0x3D
Gi5/0/0   SA       bndl    32768       0x5     0x5    0x42   0x3D
Device1#
Device1# show interface port 5
Port-channel5 is up, line protocol is up
  Hardware is GEChannel, address is 0014.a93d.4aa8 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
      Member 0 : GigabitEthernet5/0/0 , Full-duplex, 1000Mb/s <---- added to port channel
bundle
      Member 1 : GigabitEthernet7/0/0 , Full-duplex, 1000Mb/s
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Interface Port-channel5 queueing strategy: PXF First-In-First-Out
  Output queue 0/8192, 0 drops; input queue 0/150, 0 drops
  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 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    104 packets output, 8544 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collision, 0 deferred

```

```
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to remove an interface from a bundle:

```
Device1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device1(config)# interface gigabitethernet 7/0/0
Device1(config-if)# no channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:15:49.433: GigabitEthernet7/0/0 taken out of port-channel5
*Aug 20 17:15:49.557: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 5/0/0 Physical Port Link
Down
*Aug 20 17:15:50.161: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 5/0/0 Physical Port Link Down

*Aug 20 17:15:51.433: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to down
*Aug 20 17:15:52.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
changed state to down
Device1(config-if)# end
Device1#
*Aug 20 17:15:58.209: %SYS-5-CONFIG_I: Configured from console by console
Device1#
*Aug 20 17:15:59.257: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 7/0/0 Physical Port Link
Down
*Aug 20 17:15:59.257: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 7/0/0 Physical Port Link Down

Device1#
*Aug 20 17:16:01.257: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to up
*Aug 20 17:16:02.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
changed state to up
Device1# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
Channel group 5

Port      Flags    State    LACP port  Admin    Oper    Port    Port
Gi5/0/0   SA        bndl     32768      0x5      0x5     0x42    0x3D
```

Example Monitoring LACP Status

The following example shows LACP activity that you can monitor by using the **show lacp** command.

```
Device1# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
Channel group 5

Port      Flags    State    LACP port  Admin    Oper    Port    Port
Gi5/0/0   SA        bndl     32768      0x5      0x5     0x42    0x3D
Device1# show lacp 5 counters
          LACPDU      Marker      Marker Response  LACPDU
Port      Sent  Recv   Sent  Recv   Sent  Recv   Pkts Err
-----
Channel group: 5
Gi5/0/0   21    18      0     0      0     0      0
Device1# show lacp 5 internal
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
Channel group 5

Port      Flags    State    LACP port  Admin    Oper    Port    Port
Gi5/0/0   SA        bndl     32768      0x5      0x5     0x42    0x3D
Device1# show lacp 5 neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode          P - Device is in Passive mode
Channel group 5 neighbors
Partner's information:
```

Example: Displaying Port-Channel Interface Information

```

Port          Partner Partner  LACP Partner Partner  Partner Partner  Partner
Gi5/0/0       SP      32768    0011.2026.7300 11s    0x1    0x14    0x3C
Device1# show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent   Recv   Sent   Recv   Sent   Recv   Pkts Err
-----
Channel group: 5
Gi5/0/0    23     20      0      0      0      0      0
Device1# show lacp sys-id
32768,0014.a93d.4a00

```

Example: Displaying Port-Channel Interface Information

The following example shows how to display the configuration of port-channel interface 1.

```

Device# show interface port-channel 1
Port-channel1 is up, line protocol is up
Hardware is GEChannel, address is 0013.19b3.7748 (bia 0000.0000.0000)
MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
No. of active members in this channel: 2
Member 0 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet7/1/0 ,
Full-duplex, 1000Mb/s
Last input 00:00:05, output never, output hang never
Last clearing of "show interface" counters 00:04:40
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Interface Port-channel1 queueing strategy: PXF First-In-First-Out
Output queue 0/8192, 0 drops; input queue 0/75, 0 drops
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 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
3 packets output, 180 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out

```




Multichassis LACP

In Carrier Ethernet networks, various redundancy mechanisms provide resilient interconnection of nodes and networks. The choice of redundancy mechanisms depends on various factors such as transport technology, topology, single node versus entire network multihoming, capability of devices, autonomous system (AS) boundaries or service provider operations model, and service provider preferences.

Carrier Ethernet network high-availability can be achieved by employing both intra- and interchassis redundancy mechanisms. Cisco's Multichassis EtherChannel (MCEC) solution addresses the need for interchassis redundancy mechanisms, where a carrier wants to “dual home” a device to two upstream points of attachment (PoAs) for redundancy. Some carriers either cannot or will not run loop prevention control protocols in their access networks, making an alternative redundancy scheme necessary. MCEC addresses this issue with enhancements to the 802.3ad Link Aggregation Control Protocol (LACP) implementation. These enhancements are provided in the Multichassis LACP (mLACP) feature described in this document.

- [Prerequisites for mLACP, page 49](#)
- [Restrictions for mLACP, page 50](#)
- [Information About mLACP, page 51](#)
- [How to Configure mLACP, page 64](#)
- [Configuration Examples for mLACP, page 85](#)
- [Glossary, page 101](#)

Prerequisites for mLACP

- The command **lACP max-bundle** must be used on all PoAs in order to operate in PoA control and shared control modes.
 - The maximum number of links configured cannot be less than the total number of interfaces in the link aggregation group (LAG) that is connected to the PoA.
 - Each PoA may be connected to a dual-homed device (DHD) with a different number of links for the LAG (configured with a different number of maximum links).
- Each PoA must be configured using the **port-channel min-link** command with the desired minimum number of links to maintain the LAG in the active state.

- For DHD control there must be an equal number of links going to each PoA.
- The max-bundle value must equal the number of links connected locally to the PoA (no local intra-PoA active or standby protection).
- LACP fast switchover must be configured on all devices to speed convergence.

Restrictions for mLACP

- mLACP does not support Fast Ethernet.
- mLACP does not support half-duplex links.
- mLACP does not support multiple neighbors.
- Converting a port channel to mLACP can cause a service disruption.
- The maximum number of member links per LAG per PoA is restricted by the maximum number of ports per port channel, as limited by the platform.
- System priority on a DHD must be a lesser priority than on PoAs.
- MAC Tunneling Protocol (MTP) supports only one member link in a port channel.
- A port-channel or its member links may flap while LACP stabilizes.
- DHD-based control does not function when min-links is not configured.
- DHD-controlled revertive behavior with min-links is not supported.
- Brute-force failover always causes min-link failures.
- Any failure with brute-force failover behaves revertively.
- The maximum number of member links per Link Access Group (LAG) per points of attachment (PoA) is restricted by the maximum number of ports per port channel, as limited by the platform.
- The `lacp max-bundle max-links` command must be used on all the PoAs in order to operate in PoA control and shared control modes.
 - The value of the max-links variable must not be less than the total number of interfaces in the LAG, which are connected to the PoA.
 - Each PoA may be connected to the dual-homed device (DHD) with a different number of links for the LAG (and hence configured with a different value for the max-links value) variable.
- The **lacp min-bundle min-links** command has local scope only. Each PoA needs to be configured with the required minimum number of links to maintain the LAG in active state.
- When implementing the Virtual Private LAN Services (VPLS), the pseudowire states are decoupled from the attachment circuit (AC) status by default. The mLACP access state is not relayed on the VPLS pseudowires and the pseudowire continues to operate only in the decoupled mode. Coupled mode is not supported.
- mLACP and Pseudo-mLACP (P-mLACP) feature interoperation between the Cisco 7600 Series Routers and the Cisco 920 Series Aggregation Services Routers is not supported when the former is used as one PoA and the Cisco ASR 920 as another PoA in the same redundancy group.

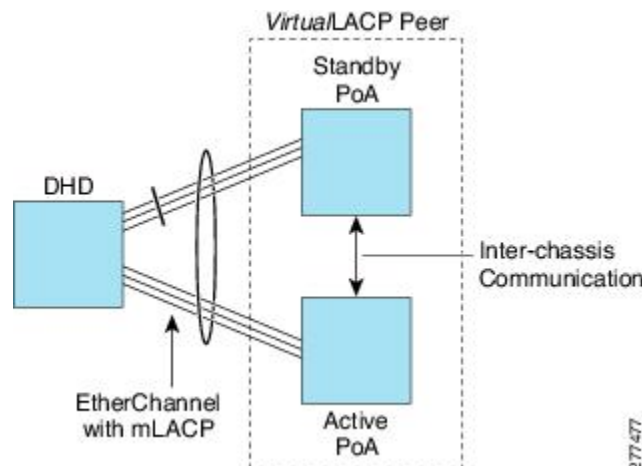
- mLACP for Layer 2 Virtual Private Network (L2VPN) is supported only with the new protocol based CLIs.
- MAC Tunneling Protocol (MTP) is not supported.
- The following commands are not supported:
 - **ethernet mac-flush notification mirp**
 - **show ethernet service instance id mac-tunnel**
 - **errdisable recovery cause mlacp**

Information About mLACP

Overview of Multichassis EtherChannel

In Multichassis EtherChannel (MCEC), the DHD is dual-homed to two upstream PoAs. The DHD is incapable of running any loop prevention control protocol such as Multiple Spanning Tree (MST). Therefore, another mechanism is required to prevent forwarding loops over the redundant setup. One method is to place the DHD's uplinks in a LAG, commonly referred to as EtherChannel. This method assumes that the DHD is capable of running only IEEE 802.3ad LACP for establishing and maintaining the LAG.

LACP, as defined in IEEE 802.3ad, is a link-level control protocol that allows the dynamic negotiation and establishment of LAGs. An extension of the LACP implementation to PoAs is required to convey to a DHD that it is connected to a single virtual LACP peer and not to two disjointed devices. This extension is called Multichassis LACP or mLACP. The figure below shows this setup.



The PoAs forming a virtual LACP peer, from the perspective of the DHD, are defined as members of a redundancy group. For the PoAs in a redundancy group to appear as a single device to the DHD, the states between them must be synchronized through the Interchassis Communication Protocol (ICCP), which provides a control-only interchassis communication channel (ICC).

In Cisco IOS Release 12.2(33)SRE, the system functions in active/standby redundancy mode. In this mode DHD uplinks that connect to only a single PoA can be active at any time. The DHD recognizes one PoA as

active and the other as standby but does not preclude a given PoA from being active for one DHD and standby for another. This capability allows two PoAs to perform load sharing for different services.

Interactions with the MPLS Pseudowire Redundancy Mechanism

The network setup shown in the figure above can be used to provide provider edge (PE) node redundancy for Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS) deployments over Multiprotocol Label Switching (MPLS). In these deployments, the uplinks of the PoAs host the MPLS pseudowires that provide redundant connectivity over the core to remote PE nodes. Proper operation of the network requires interaction between the redundancy mechanisms employed on the attachment circuits (for example, mLACP) and those employed on the MPLS pseudowires. This interaction ensures the state (active or standby) is synchronized between the attachment circuits and pseudowires for a given PoA.

RFC 4447 introduced a mechanism to signal pseudowire status via the Link Distribution Protocol (LDP) and defined a set of status codes to report attachment circuit as well as pseudowire fault information. The Preferential Forwarding Status bit (*draft-ietf-pwe3-redundancy-bit*) definition proposes to extend these codes to include two bits for pseudowire redundancy applications:

- Preferential forwarding status: active or standby
- Request pseudowire switchover

The draft also proposes two modes of operation:

- Independent mode--The local PE decides on its pseudowire status independent of the remote PE.
- Primary and secondary modes--One of the PEs determines the state of the remote side through a handshake mechanism.

For the mLACP feature, operation is based on the independent mode. By running ICC between the PoAs, only the preferential forwarding status bit is required; the request pseudowire switchover bit is not used.

The local pseudowire status (active or standby) is determined independently by the PoAs in a redundancy group and then relayed to the remote PEs in the form of a notification. Similarly, the remote PEs perform their own selection of their pseudowire status and notify the PoAs on the other side of the core.

After this exchange of local states, the pseudowires used for traffic forwarding are those selected to be active independently on both local and remote ends.

The attachment circuit redundancy mechanism determines and controls the pseudowire redundancy mechanism. mLACP determines the status of the attachment circuit on a given PoA according to the configured LACP system and port priorities, and then the status of the pseudowires on a given PoA is synchronized with that of the local attachment circuits. This synchronization guarantees that the PoA with the active attachment circuits has its pseudowires active. Similarly, the PoA with the standby attachment circuits has its pseudowires in standby mode. By ensuring that the forwarding status of the attachment circuits is synchronized with that of the pseudowires, the need to forward data between PoA nodes within a redundancy group can be avoided. This synchronization saves platform bandwidth that would otherwise be wasted on inter-PoA data forwarding in case of failures.

Redundancy Mechanism Processes

The Carrier Ethernet redundancy solution should include the following processes (and how they apply to the mLACP solution):

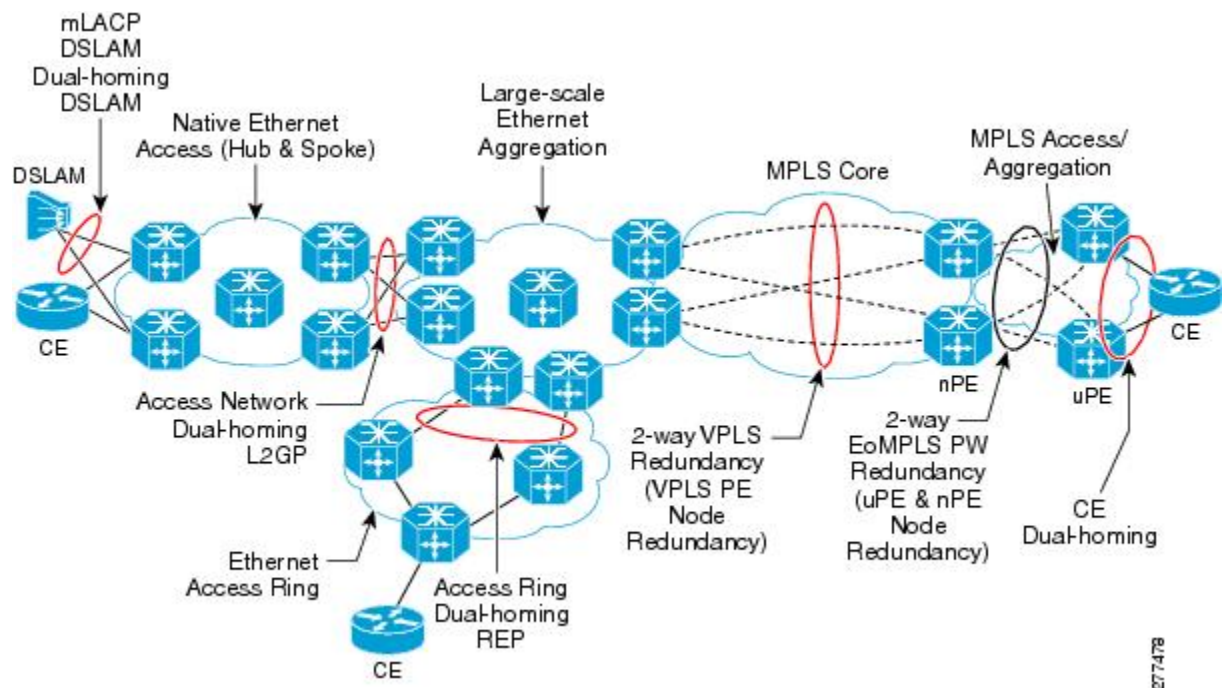
- Attachment circuit active or standby status selection--This selection can be performed by the access node or network, the aggregation node, or combination of the two. For mLACP, the attachment circuit status selection is determined through collaboration between the DHD and the PoAs.
- Pseudowire forwarding status notification--This notification is mandatory for mLACP operation in VPWS and VPLS deployments; that is, when the PoA uplinks employ pseudowire technology. When the PoAs decide on either an active or standby role, they need to signal the status of the associated pseudowires to the PEs on the far end of the network. For MPLS pseudowires, this is done using LDP.
- MAC flushing indication--This indication is mandatory for any redundancy mechanism in order to speed convergence time and eliminate potential traffic blackholing. The mLACP redundancy mechanism should be integrated with relevant 802.1Q/802.1ad/802.1ah MAC flushing mechanisms as well as MAC flushing mechanisms for VPLS.

**Note**

Blackholing occurs when incoming traffic is dropped without informing the source that the data did not reach its intended recipient. A black hole can be detected only when lost traffic is monitored.

- Active VLAN notification--For mLACP, this notification is not required as long as the PoAs follow the active/standby redundancy model.

The figure below shows redundancy mechanisms in Carrier Ethernet networks.



277478

Dual-Homed Topology Using mLACP

The mLACP feature allows the LACP state machine and protocol to operate in a dual-homed topology. The mLACP feature decouples the existing LACP implementation from the multichassis specific requirements,

allowing LACP to maintain its adherence to the IEEE 802.3ad standard. The mLACP feature exposes a single virtual instance of IEEE 802.3ad to the DHD for each redundancy group. The virtual LACP instance interoperates with the DHD according to the IEEE 802.3ad standard to form LAGs spanning two or more chassis.

LACP and 802.3ad Parameter Exchange

In IEEE 802.3ad, the concatenation of the LACP system MAC address and system priority form an LACP system ID (8 bytes). The system ID is formed by taking the two-byte system priority value as the most significant two octets of the system ID. The system MAC address makes up the remainder of the system ID (octets 3 to 8). System ID priority comparisons are based on the lower numerically valued ID.

To provide the highest LACP priority, the mLACP module communicates the system MAC address and priority values for the given redundancy group to its redundancy group peer(s) and vice versa. The mLACP then chooses the lowest system ID value among the PoAs in the given redundancy group to use as the system ID of the virtual LACP instance of the redundancy group.

Cisco IOS Release 12.2(33)SRE introduces two LACP configuration commands to specify the system MAC address and system priority used for a given redundancy group: **mlacp system-mac** *mac-address* and **mlacp system-priority** *priority-value*. These commands provide better settings to determine which side of the attachment circuit will control the selection logic of the LAG. The default value for the system MAC address is the chassis backplane default MAC address. The default value for the priority is 32768.

Port Identifier

IEEE 802.3ad uses a 4-byte port identifier to uniquely identify a port within a system. The port identifier is the concatenation of the port priority and port number (unique per system) and identifies each port in the system. Numerical comparisons between port IDs are performed by unsigned integer comparisons where the 2-byte Port Priority field is placed in the most significant two octets of the port ID. The 2-byte port number makes up the third and fourth octets. The mLACP feature coordinates the port IDs for a given redundancy group to ensure uniqueness.

Port Number

A port number serves as a unique identifier for a port within a device. The LACP port number for a port is equal to the port's ifIndex value (or is based on the slot and subslot identifiers on the Cisco 7600 router).

LACP relies on port numbers to detect rewiring. For multichassis operation, you must enter the **mlacp node-id** *node-id* command to coordinate port numbers between the two PoAs in order to prevent overlap.

Port Priority

Port priority is used by the LACP selection logic to determine which ports should be activated and which should be left in standby mode when there are hardware or software limitations on the maximum number of links allowed in a LAG. For multichassis operation in active/standby redundancy mode, the port priorities for all links connecting to the active PoA must be higher than the port priorities for links connecting to the standby PoA. These port priorities can either be guaranteed through explicit configuration or the system can automatically adjust the port priorities depending on selection criteria. For example, select the PoA with the highest port priority to be the active PoA and dynamically adjust the priorities of all other links with the same port key to an equal value.

In Cisco IOS Release 12.2(33)SRE, the mLACP feature supports only the active/standby redundancy model. The LACP port priorities of the individual member links should be the same for each link belonging to the LAG of a given PoA. To support this requirement, the **mlacp lag-priority** command is implemented in interface configuration mode in the command-line interface (CLI). This command sets the LACP port priorities for all the local member links in the LAG. Individual member link LACP priorities (configured by the **lacp port-priority** command) are ignored on links belonging to mLACP port channels.

The **mlacp lag-priority** command may also be used to force a PoA failover during operation in the following two ways:

- Set the active PoA's LAG priority to a value greater than the LAG priority on the standby PoA. This setting results in the quickest failover because it requires the fewest LACP link state transitions on the standby links before they turn active.
- Set the standby PoA's LAG priority to a value numerically less than the LAG priority on the active PoA. This setting results in a slightly longer failover time because standby links have to signal OUT_OF_SYNC to the DHD before the links can be brought up and go active.

In some cases, the operational priority and the configured priority may differ when using dynamic port priority management to force failovers. In this case, the configured version will not be changed unless the port channel is operating in nonrevertive mode. Enter the **show lacp multichassis port-channel** command to view the current operational priorities. The configured priority values can be displayed by using the **show running-config** command.

Multichassis Considerations

Because LACP is a link layer protocol, all messages exchanged over a link contain information that is specific and local to that link. The exchanged information includes:

- System attributes--priority and MAC address
- Link attributes--port key, priority, port number, and state

When extending LACP to operate over a multichassis setup, synchronization of the protocol attributes and states between the two chassis is required.

System MAC Address

LACP relies on the system MAC address to determine the identity of the remote device connected over a particular link. Therefore, to mask the DHD from its connection to two disjointed devices, coordination of the system MAC address between the two PoAs is essential. In Cisco IOS software, the LACP system MAC address defaults to the ROM backplane base MAC address and cannot be changed by configuration. For multichassis operation the following two conditions are required:

- System MAC address for each PoA should be communicated to its peer--For example, the PoAs elect the MAC address with the lower numeric value to be the system MAC address. The arbitration scheme must resolve to the same value. Choosing the lower numeric MAC address has the advantage of providing higher system priority.
- System MAC address is configurable--The system priority depends, in part, on the MAC address, and a service provider would want to guarantee that the PoAs have higher priority than the DHD (for example, if both DHD and PoA are configured with the same system priority and the service provider has no control over DHD). A higher priority guarantees that the PoA port priorities take precedence over the

DHD's port priority configuration. If you configure the system MAC address, you must ensure that the addresses are uniform on both PoAs; otherwise, the system will automatically arbitrate the discrepancy, as when a default MAC address is selected.

System Priority

LACP requires that a system priority be associated with every device to determine which peer's port priorities should be used by the selection logic when establishing a LAG. In Cisco IOS software, this parameter is configurable through the CLI. For multichassis operation, this parameter is coordinated by the PoAs so that the same value is advertised to the DHD.

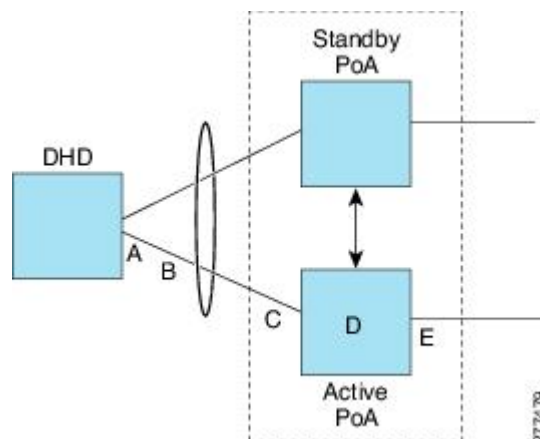
Port Key

The port key indicates which links can form a LAG on a given system. The key is locally significant to an LACP system and need not match the key on an LACP peer. Two links are candidates to join the same LAG if they have the same key on the DHD and the same key on the PoAs; however, the key on the DHD is not required to be the same as the key on the PoAs. Given that the key is configured according to the need to aggregate ports, there are no special considerations for this parameter for multichassis operation.

Failure Protection Scenarios

The mLACP feature provides network resiliency by protecting against port, link, and node failures. These failures can be categorized into five types. The figure below shows the failure points in a network, denoted by the letters A through E.

- A--Failure of the uplink port on the DHD
- B--Failure of the Ethernet link
- C--Failure of the downlink port on the active PoA
- D--Failure of the active PoA node
- E--Failure of the active PoA uplinks



When any of these faults occur, the system reacts by triggering a switchover from the active PoA to the standby PoA. The switchover involves failing over the PoA's uplinks and downlinks simultaneously.

Failure points A and C are port failures. Failure point B is an Ethernet link failure and failure point D is a node failure. Failure point E can represent one of four different types of uplink failures when the PoAs connect to an MPLS network:

- Pseudowire failure--Monitoring individual pseudowires (for example, using VCCV-BFD) and, upon a pseudowire failure, declare uplink failure for the associated service instances.
- Remote PE IP path failure--Monitoring the IP reachability to the remote PE (for example, using IP Route-Watch) and, upon route failure, declare uplink failure for all associated service instances.
- LSP failure--Monitoring the LSP to a given remote PE (for example, using automated LSP-Ping) and, upon LSP failure, declare uplink failure for all associated service instances.
- PE isolation--Monitoring the physical core-facing interfaces of the PE. When all of these interfaces go down, the PE effectively becomes isolated from the core network, and the uplink failure is declared for all affected service instances.

As long as the IP/MPLS network employs native redundancy and resiliency mechanisms such as MPLS fast reroute (FRR), the mLACP solution is sufficient for providing protection against PE isolation. Pseudowire, LSP, and IP path failures are managed by the native IP/MPLS protection procedures. That is, interchassis failover via mLACP is triggered only when a PE is completely isolated from the core network, because native IP/MPLS protection mechanisms are rendered useless. Therefore, failure point E is used to denote PE isolation from the core network.

**Note**

The set of core-facing interfaces that should be monitored are identified by explicit configuration. The set of core-facing interfaces must be defined independently per redundancy group. Failure point E (unlike failure point A, B, or C) affects and triggers failover for all the multichassis LAGs configured on a given PoA.

Operational Variants

LACP provides a mechanism by which a set of one or more links within a LAG are placed in standby mode to provide link redundancy between the devices. This redundancy is normally achieved by configuring more ports with the same key than the number of links a device can aggregate in a given LAG (due to hardware or software restrictions, or due to configuration). For active/standby redundancy, two ports are configured with the same port key, and the maximum number of allowed links in a LAG is configured to be 1. If the DHD and PoAs are all capable of restricting the number of links per LAG by configuration, three operational variants are possible.

DHD-based Control

The DHD is configured to limit the maximum number of links per bundle to one, whereas the PoAs are configured to limit the maximum number of links per bundle to greater than one. Thus, the selection of the active/standby link is the responsibility of the DHD. Which link is designated active and which is marked standby depends on the relative port priority, as configured on the system with the higher system priority. A PoA configured with a higher system priority can still determine the selection outcome. The DHD makes the selection and places the link with lower port priority in standby mode.

To accommodate DHD-controlled failover, the DHD must be configured with the max-bundle value equal to a number of links (L), where L is the fewest number of links connecting the DHD to a PoA. The max-bundle value restricts the DHD from bundling links to both PoAs at the same time (active/active). Although the DHD controls the selection of active/standby links, the PoA can still dictate the individual member link priorities by configuring the PoA's virtual LACP instance with a lower system priority value than the DHD's system priority.

The DHD control variant must be used with a PoA minimum link threshold failure policy where the threshold is set to L (same value for L as described above). A minimum link threshold must be configured on each of the PoAs because an A, B, or C link failure that does not trigger a failover (minimum link threshold is still satisfied) causes the DHD to add one of the standby links going to the standby PoA to the bundle. This added link results in the unsupported active/active scenario.


Note

DHD control does not use the mLACP hot-standby state on the standby PoA, which results in higher failover times than the other variants.

DHD control eliminates the split brain problem on the attachment circuit side by limiting the DHD's attempts to bundle all the links.

PoA Control

In PoA control, the PoA is configured to limit the maximum number of links per bundle to be equal to the number of links (L) going to the PoA. The DHD is configured with that parameter set to some value greater than L. Thus, the selection of the active/standby links becomes the responsibility of the PoA.

Shared Control (PoA and DHD)

In shared control, both the DHD and the PoA are configured to limit the maximum number of links per bundle to L--the number of links going to the PoA. In this configuration, each device independently selects the active/standby link. Shared control is advantageous in that it limits the split-brain problem in the same manner as DHD control, and shared control is not susceptible to the active/active tendencies that are prevalent in DHD control. A disadvantage of shared control is that the failover time is determined by both the DHD and the PoA, each changing the standby links to SELECTED and waiting for each of the WAIT_WHILE_TIMERS to expire before moving the links to IN_SYNC. The independent determination of failover time and change of link states means that both the DHD and PoAs need to support the LACP fast-switchover feature in order to provide a failover time of less than one second.

mLACP Failover

The mLACP forces a PoA failover to the standby PoA when one of the following failures occurs:

- Failure of the DHD uplink port, Ethernet link, or downlink port on the active PoA--A policy failover is triggered via a configured failover policy and is considered a forced failover. In Cisco IOS Release 12.2(33)SRE, the only option is the configured minimum bundle threshold. When the number of active and SELECTED links to the active PoA goes below the configured minimum threshold, mLACP forces a failover to the standby PoA's member links. This minimum threshold is configured using the **port-channel min-links** command in interface configuration mode. The PoAs determine the failover independent of the operational control variant in use.

- Failure of the active PoA--This failure is detected by the standby PoA. mLACP automatically fails over to standby because mLACP on the standby PoA is notified of failure via ICRM and brings up its local member links. In the DHD-controlled variant, this failure looks the same as a total member link failure, and the DHD activates the standby links.
- Failure of the active PoA uplinks--mLACP is notified by ICRM of PE isolation and relinquishes its active member links. This failure is a “forced failover” and is determined by the PoAs independent of the operational control variant in use.

Dynamic Port Priority

The default failover mechanism uses dynamic port priority changes on the local member links to force the LACP selection logic to move the required standby link(s) to the SELECTED and Collecting_Distributing state. This state change occurs when the LACP actor port priority values for all affected member links on the currently active PoA are changed to a higher numeric value than the standby PoA's port priority (which gives the standby PoA ports a higher claim to bundle links). Changing the actor port priority triggers the transmission of an mLACP Port Config Type-Length-Value (TLV) message to all peers in the redundancy group. These messages also serve as notification to the standby PoA(s) that the currently active PoA is attempting to relinquish its role. The LACP then transitions the standby link(s) to the SELECTED state and moves all the currently active links to STANDBY.

Dynamic port priority changes are not automatically written back to the running configuration or to the NVRAM configuration. If you want the current priorities to be used when the system reloads, the **mlacp lag-priority** command must be used and the configuration must be saved.

Revertive and Nonrevertive Modes

Dynamic port priority functionality is used by the mLACP feature to provide both revertive mode and nonrevertive mode. The default operation is revertive, which is the default behavior in single chassis LACP. Nonrevertive mode can be enabled on a per port-channel basis by using the **lacp failover non-revertive** command in interface configuration mode. In Cisco IOS Release 12.2(33)SRE this command is supported only for mLACP.

Nonrevertive mode is used to limit failover and, therefore, possible traffic loss. Dynamic port priority changes are utilized to ensure that the newly activated PoA remains active after the failed PoA recovers.

Revertive mode operation forces the configured primary PoA to return to active state after it recovers from a failure. Dynamic port priority changes are utilized when necessary to allow the recovering PoA to resume its active role.

Brute Force Shutdown

A brute-force shutdown is a forced failover mechanism to bring down the active physical member link interface(s) for the given LAG on the PoA that is surrendering its active status. This mechanism does not depend on the DHD's ability to manage dynamic port priority changes and compensates for deficiencies in the DHD's LACP implementation.

The brute-force shutdown changes the status of each member link to ADMIN_DOWN to force the transition of the standby links to the active state. Note that this process eliminates the ability of the local LACP implementation to monitor the link state.

The brute-force shutdown operates in revertive mode, so dynamic port priorities cannot be used to control active selection. The brute-force approach is configured by the **lacp failover brute-force** command in interface configuration mode. This command is not allowed in conjunction with a nonrevertive configuration.

Peer Monitoring with Interchassis Redundancy Manager

There are two ways in which a peer can be monitored with Interchassis Redundancy Manager (ICRM):

- Routewatch (RW)--This method is the default.
- Bidirectional Forwarding Detection (BFD)--You must configure the redundancy group with the **monitor peer bfd** command.



Note

For stateful switchover (SSO) deployments (with redundant support in the chassis), BFD monitoring and a static route for the ICCP connection are required to prevent “split brain” after an SSO failover.

For each redundancy group, for each peer (member IP), a monitoring adjacency is created. If there are two peers with the same IP address, the adjacency is shared regardless of the monitoring mode. For example, if redundancy groups 1 and 2 are peered with member IP 10.10.10.10, there is only one adjacency to 10.10.10.10, which is shared in both redundancy groups. Furthermore, redundancy group 1 can use BFD monitoring while redundancy group 2 is using RW.



Note

BFD is completely dependent on RW--there must be a route to the peer for ICRM to initiate BFD monitoring. BFD implies RW and sometimes the status of the adjacency may seem misleading but is accurately representing the state. Also, if the route to the peer PoA is not through the directly connected (back-to-back) link between the systems, BFD can give misleading results.

An example of output from the **show redundancy interface** command follows:

```
Device# show redundancy interface
Redundancy Group 1 (0x1)
  Applications connected: mLACP
  Monitor mode: Route-watch
  member ip: 201.0.0.1 'mlacp-201', CONNECTED
  Route-watch for 201.0.0.1 is UP
  mLACP state: CONNECTED
ICRM fast-failure detection neighbor table
IP Address      Status Type Next-hop IP      Interface
=====
201.0.0.1      UP      RW
```

To interpret the adjacency status displayed by the **show redundancy interchassis** command, refer to the table below.

Table 3: Status Information from the show redundancy interchassis command

Adjacency Type	Adjacency Status	Meaning
RW	DOWN	RW or BFD is configured, but there is no route for the given IP address.

Adjacency Type	Adjacency Status	Meaning
RW	UP	RW or BFD is configured. RW is up, meaning there is a valid route to the peer. If BFD is configured and the adjacency status is UP, BFD is probably not configured on the interface of the route's adjacency.
BFD	DOWN	BFD is configured. A route exists and the route's adjacency is to an interface that has BFD enabled. BFD is started but the peer is down. The DOWN status can be because the peer is not present or BFD is not configured on the peer's interface.
BFD	UP	BFD is configured and operational.

**Note**

If the adjacency type is “BFD,” RW is UP regardless of the BFD status.

MAC Flushing Mechanisms

When mLACP is used to provide multichassis redundancy in multipoint bridged services (for example, VPLS), there must be a MAC flushing notification mechanism in order to prevent potential traffic blackholing.

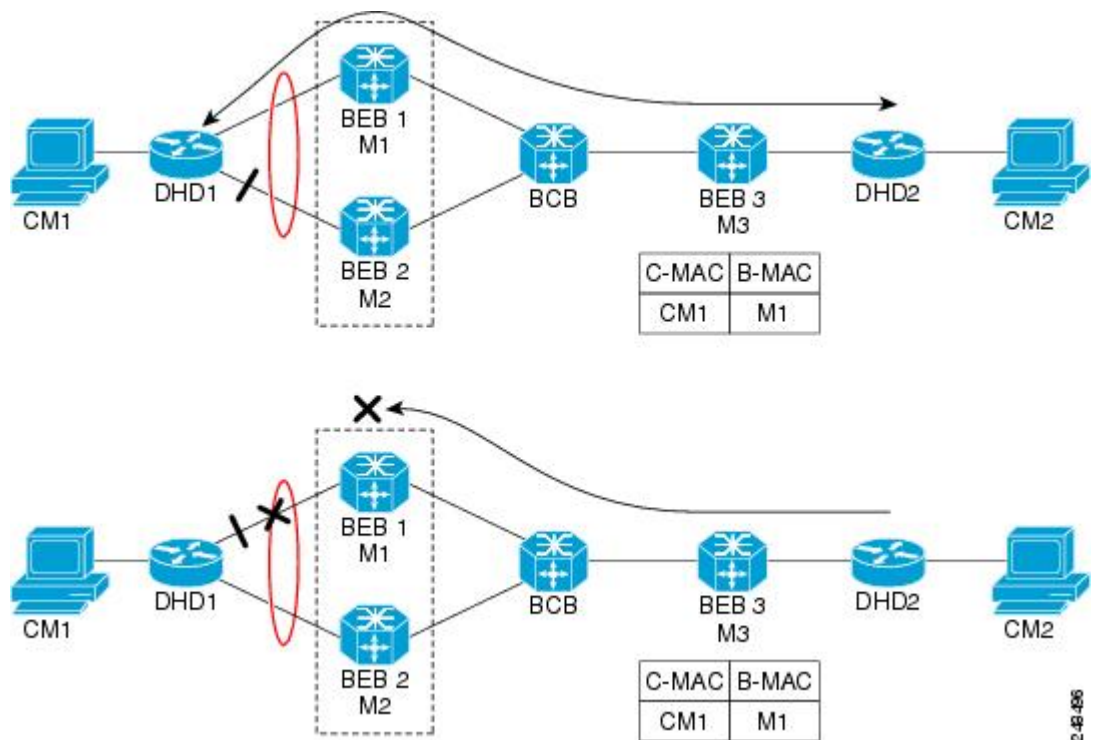
At the failover from a primary PoA to a secondary PoA, a service experiences traffic blackholing when the DHD in question remains inactive and while other remote devices in the network are attempting to send traffic to that DHD. Remote bridges in the network have stale MAC entries pointing to the failed PoA and direct traffic destined to the DHD to the failed PoA, where the traffic is dropped. This blackholing continues until the remote devices age out their stale MAC address table entries (which typically takes five minutes). To prevent this anomaly, the newly active PoA, which has taken control of the service, transmits a MAC flush notification message to the remote devices in the network to flush their stale MAC address entries for the service in question.

The exact format of the MAC flushing message depends on the nature of the network transport: native 802.1Q/802.1ad Ethernet, native 802.1ah Ethernet, VPLS, or provider backbone bridge (PBB) over VPLS. Furthermore, in the context of 802.1ah, it is important to recognize the difference between mechanisms used for customer-MAC (C-MAC) address flushing versus bridge-MAC (B-MAC) address flushing.

The details of the various mechanisms are discussed in the following sections.

Multiple I-SID Registration Protocol

Multiple I-SID Registration Protocol (MIRP) is enabled by default on 802.1ah service instances. The use of MIRP in 802.1ah networks is shown in the figure below.



Device DHD1 is dual-homed to two 802.1ah backbone edge bridges (BEB1 and BEB2). Assume that initially the primary path is through BEB1. In this configuration BEB3 learns that the host behind DHD1 (with MAC address CM1) is reachable via the destination B-MAC M1. If the link between DHD1 and BEB1 fails and the host behind DHD1 remains inactive, the MAC cache tables on BEB3 still refer to the BEB1 MAC address even though the new path is now via BEB2 with B-MAC address M2. Any bridged traffic destined from the host behind DHD2 to the host behind DHD1 is wrongfully encapsulated with B-MAC M1 and sent over the MAC tunnel to BEB1, where the traffic blackholes.

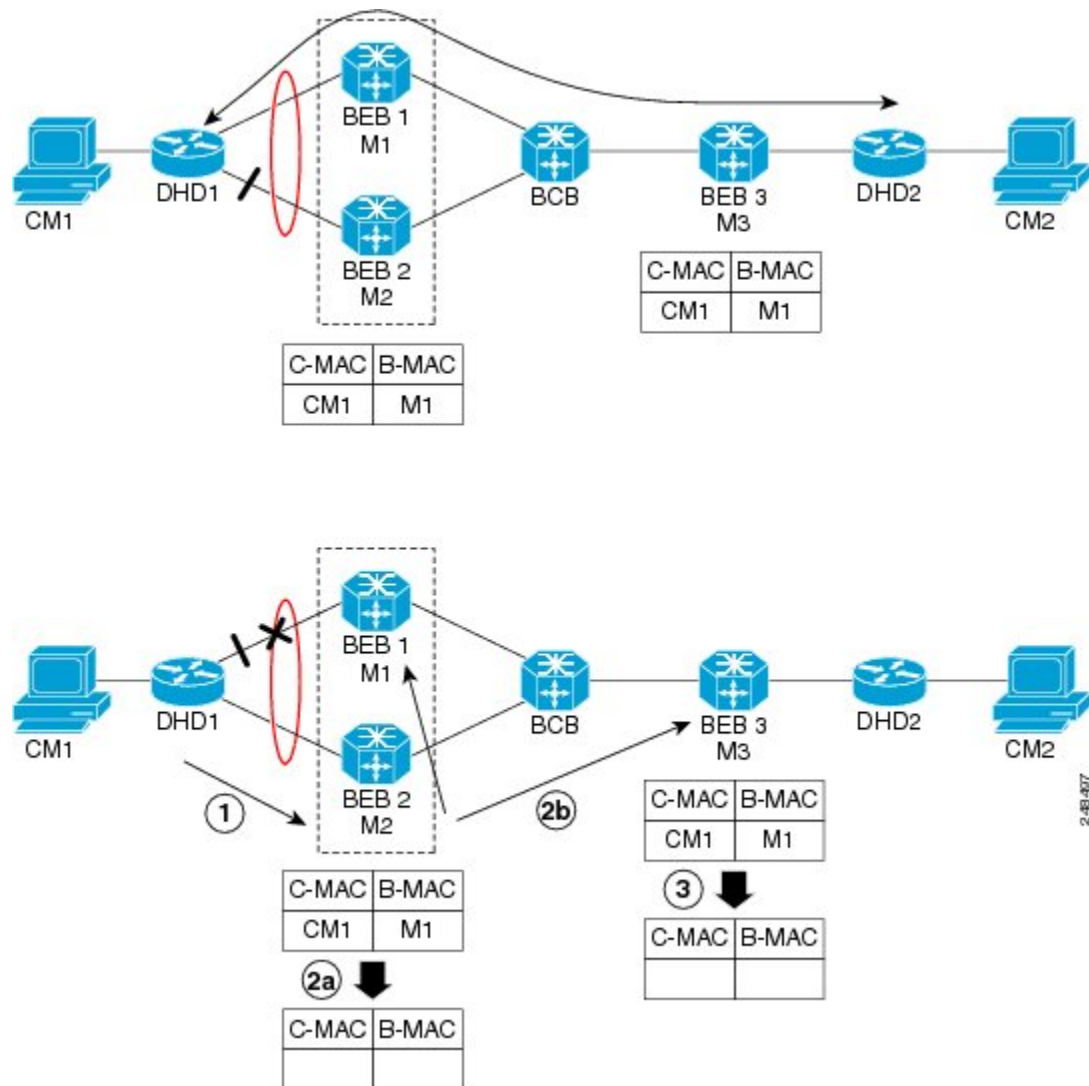
To circumvent the traffic blackholing problem when the link between DHD1 and BEB1 fails, BEB2 performs two tasks:

- Flushes its own MAC address table for the service or services in question.
- Transmits an MIRP message on its uplink to signal the far end BEB (BEB3) to flush its MAC address table. Note that the MIRP message is transparent to the backbone core bridges (BCBs). The MIRP message is processed on a BEB because only BCBs learn and forward based on B-MAC addresses and they are transparent to C-MAC addresses.


Note

MIRP triggers C-MAC address flushing for both native 802.1ah and PBB over VPLS.

The figure below shows the operation of the MIRP.



The MIRP has not been defined in IEEE but is expected to be based on the IEEE 802.1ak Multiple Registration Protocol (MRP). MRP maintains a complex finite state machine (FSM) for generic attribute registration. In the case of MIRP, the attribute is an I-SID. As such, MIRP provides a mechanism for BEBs to build and prune a per I-SID multicast tree. The C-MAC flushing notification capability of MIRP is a special case of attribute registration in which the device indicates that an MIRP declaration is “new,” meaning that this notification is the first time a BEB is declaring interest in a particular I-SID.

LDP MAC Address Withdraw

When the mLACP feature is used for PE redundancy in traditional VPLS (that is, not PBB over VPLS), the MAC flushing mechanism is based on the LDP MAC Address Withdraw message as defined in RFC 4762.

The required functional behavior is as follows: Upon a failover from the primary PoA to the standby PoA, the standby PoA flushes its local MAC address table for the affected services and generates the LDP MAC Address Withdraw messages to notify the remote PEs to flush their own MAC address tables. One message is generated for each pseudowire in the affected virtual forwarding instances (VFIs).

How to Configure mLACP

Configuring Interchassis Group and Basic mLACP Commands

Perform this task to set up the communication between multiple PoAs and to configure them in the same group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **interchassis group** *group-id*
5. **monitor peer bfd**
6. **member ip** *ip-address*
7. **mlacp node-id** *node-id*
8. **mlacp system-mac** *mac-address*
9. **mlacp system-priority** *priority-value*
10. **backbone interface** *type number*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	redundancy Example: Router(config)# redundancy	Enters redundancy configuration mode.

	Command or Action	Purpose
Step 4	interchassis group <i>group-id</i> Example: Router(config-red)# interchassis group 50	Configures an interchassis group within the redundancy configuration mode and enters interchassis redundancy mode.
Step 5	monitor peer bfd Example: Router(config-r-ic)# monitor peer bfd	Configures the BFD option to monitor the state of the peer. The default option is route-watch.
Step 6	member ip <i>ip-address</i> Example: Router(config-r-ic)# member ip 172.3.3.3	Configures the IP address of the mLACP peer member group.
Step 7	mlacp node-id node-id Example: Router(config-r-ic)# mlacp node-id 5	Defines the node ID used in the LACP Port ID field by this member of the mLACP redundancy group. <ul style="list-style-type: none"> The valid range is 0 to 7, and the value should be different from the peer values.
Step 8	mlacp system-mac mac-address Example: Router(config-r-ic)# mlacp system-mac aa12.be45.d799	Defines and advertises the system MAC address value to the mLACP members of the redundancy group for arbitration. <ul style="list-style-type: none"> The format of the <i>mac-address</i> argument must be in standard MAC address format: aabb.ccdd.eeff.
Step 9	mlacp system-priority <i>priority-value</i> Example: Router(config-r-ic)# mlacp system-priority 100	Defines the system priority advertised to the other mLACP members of the redundancy group. <ul style="list-style-type: none"> System priority values are 1 to 65535. Default value is 32768. The assigned values should be lower than the DHD.
Step 10	backbone interface <i>type number</i> Example: Router(config-r-ic)# backbone interface GigabitEthernet2/3	Defines the backbone interface for the mLACP configuration.
Step 11	end Example: Router(config-r-ic)# end	Returns the CLI to privileged EXEC mode.

Configuring the mLACP Interchassis Group and Other Port-Channel Commands

Perform this task to set up mLACP attributes specific to a port channel. The **mlacp interchassis group** command links the port-channel interface to the interchassis group that was created in the previous [Configuring Interchassis Group and Basic mLACP Commands](#), on page 64.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *port-channel- number*
4. **lacp max-bundle** *max-bundles*
5. **lacp failover** {**brute-force**|**non-revertive**}
6. **exit**
7. **redundancy**
8. **interchassis group** *group-id*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface port-channel <i>port-channel- number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.
Step 4	lacp max-bundle <i>max-bundles</i> Example: Router(config-if)# lacp max-bundle 4	Configures the max-bundle links that are connected to the PoA. The value of the <i>max-bundles</i> argument should not be less than the total number of links in the LAG that are connected to the PoA. <ul style="list-style-type: none"> • Determines whether the redundancy group is under DHD control, PoA control, or both.

	Command or Action	Purpose
		<ul style="list-style-type: none"> Range is 1 to 8. Default value is 8.
Step 5	lacp failover {brute-force non-revertive} Example: <pre>Router(config-if)# lacp failover brute-force</pre>	Sets the mLACP switchover to nonrevertive or brute force. This command is optional. <ul style="list-style-type: none"> Default value is revertive (with 180-second delay). If you configure brute force, a minimum link failure for every mLACP failure occurs or the dynamic lag priority value is modified.
Step 6	exit Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.
Step 7	redundancy Example: <pre>Router(config)# redundancy</pre>	Enters redundancy configuration mode.
Step 8	interchassis group group-id Example: <pre>Router(config-red)# interchassis group 230</pre>	Specifies that the port channel is an mLACP port channel. The <i>group-id</i> should match the configured redundancy group.
Step 9	end Example: <pre>Router(config-r-ic)# end</pre>	Returns the CLI to privileged EXEC mode.

Configuring Redundancy for VPWS

Perform this task to provide Layer 2 VPN service redundancy for VPWS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *pw-class-name*
4. **encapsulation mpls**
5. **status peer topology dual-homed**
6. **exit**
7. **interface port-channel** *port-channel-number*
8. **no ip address**
9. **lACP fast-switchover**
10. **lACP max-bundle** *max-bundles*
11. **exit**
12. **redundancy**
13. **interchassis group** *group-id*
14. **exit**
15. **exit**
16. **interface port-channel** *port-channel-number*
17. **service instance** *id* **ethernet** [*evc-name*]
18. **encapsulation dot1q** *vlan-id* [, *vlan-id*[- *vlan-id*]] [**native**]
19. **exit**
20. **xconnect** *peer-ip-address* *vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
21. **backup peer** *peer-router-ip-addr* *vcid* [**pw-class** *pw-class-name*] [**priority value**]
22. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	pseudowire-class <i>pw-class-name</i> Example: Router(config)# pseudowire-class ether-pw	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 4	encapsulation mpls Example: Router(config-pw-class)# encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.
Step 5	status peer topology dual-homed Example: Router(config-pw-class)# status peer topology dual-homed	Enables the reflection of the attachment circuit status onto both the primary and secondary pseudowires. This condition is necessary if the peer PEs are connected to a dual-homed device.
Step 6	exit Example: Router(config-pw-class)# exit	Exits pseudowire class configuration mode.
Step 7	interface port-channel <i>port-channel-number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.
Step 8	no ip address Example: Router(config-if)# no ip address	Specifies that the VLAN interface does not have an IP address assigned to it.
Step 9	lacp fast-switchover Example: Router(config-if)# lacp fast-switchover	Enables LACP 1-to-1 link redundancy.
Step 10	lacp max-bundle <i>max-bundles</i> Example: Router(config-if)# lacp max-bundle 4	Configures the max-bundle links that are connected to the PoA. The value of the <i>max-bundles</i> argument should not be less than the total number of links in the LAG that are connected to the PoA. <ul style="list-style-type: none"> • Determines whether the redundancy group is under DHD control, PoA control, or both. • Range is 1 to 8. Default value is 8.

	Command or Action	Purpose
Step 11	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 12	redundancy Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 13	interchassis group <i>group-id</i> Example: Router(config-red)# interchassis group 230	Specifies that the port channel is an mLACP port channel. <ul style="list-style-type: none"> The <i>group-id</i> should match the configured redundancy group.
Step 14	exit Example: Router(config-r-ic)# exit	Exits interchassis redundancy mode.
Step 15	exit Example: Router(config-red)# exit	Exits redundancy configuration mode.
Step 16	interface port-channel <i>port-channel-number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.
Step 17	service instance <i>id</i> ethernet [<i>evc-name</i>] Example: Router(config-if)# service instance 1 ethernet	Configures an Ethernet service instance.
Step 18	encapsulation dot1q <i>vlan-id</i> [, <i>vlan-id</i> [- <i>vlan-id</i>]] [native] Example: Router(config-if-srv)# encapsulation dot1q 100	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.

	Command or Action	Purpose
Step 19	exit Example: <pre>Router(config-if-srv)# exit</pre>	Exits service instance configuration mode.
Step 20	xconnect <i>peer-ip-address</i> <i>vc-id</i> { encapsulation mpls pw-class <i>pw-class-name</i> } [pw-class <i>pw-class-name</i>] [sequencing { transmit receive both }] Example: <pre>Router(config-if)# xconnect 10.0.3.201 123 pw-class ether-pw</pre>	Binds an attachment circuit to a pseudowire.
Step 21	backup peer <i>peer-router-ip-addr</i> <i>vcid</i> [pw-class <i>pw-class-name</i>] [priority <i>value</i>] Example: <pre>Router(config-if)# backup peer 10.1.1.1 123 pw-class ether-pw</pre>	Specifies a redundant peer for a pseudowire virtual circuit.
Step 22	end Example: <pre>Router(config-if)# end</pre>	Returns the CLI to privileged EXEC mode.

Configuring Redundancy for VPLS

Coupled and Decoupled Modes for VPLS

VPLS can be configured in either coupled mode or decoupled mode. Coupled mode is when at least one attachment circuit in VFI changes state to active, all pseudowires in VFI advertise active. When all attachment circuits in VFI change state to standby, all pseudowires in VFI advertise standby mode. See the figure below.



VPLS decoupled mode is when all pseudowires in the VFI are always active and the attachment circuit state is independent of the pseudowire state. This mode provides faster switchover time when a platform does not

support pseudowire status functionality, but extra flooding and multicast traffic will be dropped on the PE with standby attachment circuits. See the figure below.



Steps for Configuring Redundancy for VPLS

Perform the following task to configure redundancy for VPLS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 vfi *name* manual**
4. **vpn id *vpn-id***
5. **status decoupled**
6. **neighbor *neighbor ip-address* vc-id {encapsulation mpls | pw-class *pw-class-name*}**
7. **exit**
8. **interface port-channel *port-channel- number***
9. **no ip address**
10. **lacp fast-switchover**
11. **lacp max-bundle *max-bundles***
12. **exit**
13. **redundancy**
14. **interchassis group *group-id***
15. **exit**
16. **exit**
17. **interface port-channel *port-channel- number***
18. **service instance *id* ethernet [*evc-name*]**
19. **encapsulation dot1q *vlan-id* [, *vlan-id*[- *vlan-id*]] [native]**
20. **bridge-domain *bridge-id* [split-horizon [group *group-id*]]**
21. **exit**
22. **interface vlan *vlanid***
23. **no ip address**
24. **xconnect vfi *vfi-name***
25. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	l2 vfi name manual Example: Router(config)# l2 vfi vfi1 manual	Establishes a Layer 2 VFI between two separate networks and enters VFI configuration mode.
Step 4	vpn id vpn-id Example: Router(config-vfi)# vpn id 100	Sets or updates a Virtual Private Network (VPN) ID on a VPN routing and forwarding (VRF) instance.
Step 5	status decoupled Example: Router(config-vfi)# status decoupled	(Optional) Enables decoupled mode. The state of the attachment circuits on the user-facing Provider Edge (uPE) is decoupled from the state of the pseudowires. The mLACP controls the state of the attachment circuits.
Step 6	neighbor neighbor ip-address vc-id {encapsulation mpls pw-class pw-class-name} Example: Router(config-vfi)# neighbor 10.1.1.1 50 encapsulation mpls	Specifies the routers that should form a VFI connection. <ul style="list-style-type: none"> • Repeat this command for each neighbor.
Step 7	exit Example: Router(config-vfi)# exit	Exits VFI configuration mode and returns to global configuration mode.
Step 8	interface port-channel port-channel- number Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.

	Command or Action	Purpose
Step 9	no ip address Example: Router(config-if)# no ip address	Specifies that the VLAN interface does not have an IP address assigned to it.
Step 10	lacp fast-switchover Example: Router(config-if)# lacp fast-switchover	Enables LACP 1-to-1 link redundancy.
Step 11	lacp max-bundle <i>max-bundles</i> Example: Router(config-if)# lacp max-bundle 2	Configures the max-bundle links that are connected to the PoA. The value of the <i>max-bundles</i> argument should not be less than the total number of links in the LAG that are connected to the PoA. <ul style="list-style-type: none"> • Determines whether the redundancy group is under DHD control, PoA control, or both. • Range is 1 to 8. Default value is 8.
Step 12	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 13	redundancy Example: Router(config)# redundancy	<ul style="list-style-type: none"> • Enters redundancy configuration mode.
Step 14	interchassis group <i>group-id</i> Example: Router(config-red)# interchassis group 230	Specifies that the port channel is an mLACP port-channel. <ul style="list-style-type: none"> • The <i>group-id</i> should match the configured redundancy group.
Step 15	exit Example: Router(config-r-ic)# exit	Exits interchassis redundancy mode.
Step 16	exit Example: Router(config-red)# exit	Exits redundancy configuration mode.

	Command or Action	Purpose
Step 17	interface port-channel <i>port-channel- number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.
Step 18	service instance <i>id</i> ethernet [<i>evc-name</i>] Example: Router(config-if)# service instance 1 ethernet	Configures an Ethernet service instance and enters Ethernet service configuration mode.
Step 19	encapsulation dot1q <i>vlan-id</i> [, <i>vlan-id</i> [- <i>vlan-id</i>]] [native] Example: Router(config-if-srv)# encapsulation dot1q 100	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 20	bridge-domain <i>bridge-id</i> [split-horizon [group <i>group-id</i>]] Example: Router(config-if-srv)# bridge-domain 200	Configures the bridge domain. Binds the service instance to a bridge domain instance where <i>domain-number</i> is the identifier for the bridge domain instance.
Step 21	exit Example: Router(config-if-srv)# exit	Exits service instance configuration mode.
Step 22	interface vlan <i>vlanid</i> Example: Router(config-if)# interface vlan 200	Creates a dynamic switch virtual interface (SVI).
Step 23	no ip address Example: Router(config-if)# no ip address	Specifies that the VLAN interface does not have an IP address assigned to it.
Step 24	xconnect vfi <i>vfi-name</i> Example: Router(config-if)# xconnect vfi vfi-16	Specifies the Layer 2 VFI that you are binding to the VLAN port.

	Command or Action	Purpose
Step 25	end Example: Router(config-if)# end	Returns the CLI to privileged EXEC mode.

Configuring Hierarchical VPLS

Perform this task to configure Hierarchical VPLS (H-VPLS).

SUMMARY STEPS

1. enable
2. configure terminal
3. pseudowire-class *pw-class-name*
4. encapsulation mpls
5. status peer topology dual-homed
6. status decoupled
7. exit
8. interface port-channel *port-channel- number*
9. no ip address
10. lacp fast-switchover
11. lacp max-bundle *max-bundles*
12. exit
13. redundancy
14. interchassis group *group-id*
15. exit
16. exit
17. interface port-channel *port-channel- number*
18. service instance *id* ethernet [*evc-name*]
19. encapsulation dot1q *vlan-id* [, *vlan-id*[- *vlan-id*]] [native]
20. exit
21. xconnect *peer-ip-address* *vc-id* {encapsulation mpls | pw-class *pw-class-name*} [pw-class *pw-class-name*] [sequencing {transmit | receive | both}]
22. backup peer *peer-router-ip-addr* *vcid* [pw-class *pw-class-name*] [priority *value*]
23. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	pseudowire-class <i>pw-class-name</i> Example: Router(config)# pseudowire-class ether-pw	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 4	encapsulation mpls Example: Router(config-pw-class)# encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.
Step 5	status peer topology dual-homed Example: Router(config-pw-class)# status peer topology dual-homed	Enables the reflection of the attachment circuit status onto both the primary and secondary pseudowires. This configuration is necessary if the peer PEs are connected to a dual-homed device.
Step 6	status decoupled Example: Router(config-pw-class)# status decoupled	(Optional) Enables decoupled mode. The state of the attachment circuits on the uPE is decoupled from the state of the pseudowires. The mLACP controls the state of the attachment circuits.
Step 7	exit Example: Router(config-pw-class)# exit	Exits pseudowire class configuration mode and returns to global configuration mode.
Step 8	interface port-channel <i>port-channel- number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.

	Command or Action	Purpose
Step 9	no ip address Example: Router(config-if)# no ip address	Specifies that the VLAN interface does not have an IP address assigned to it.
Step 10	lacp fast-switchover Example: Router(config-if)# lacp fast-switchover	Enables LACP 1-to-1 link redundancy.
Step 11	lacp max-bundle <i>max-bundles</i> Example: Router(config-if)# lacp max-bundle 4	Configures the max-bundle links that are connected to the PoA. The value of the <i>max-bundles</i> argument should not be less than the total number of links in the LAG that are connected to the PoA. <ul style="list-style-type: none"> • Determines whether the redundancy group is under DHD control, PoA control, or both. • Range is 1 to 8. Default value is 8.
Step 12	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 13	redundancy Example: Router(config)# redundancy	Enters redundancy configuration mode.
Step 14	interchassis group <i>group-id</i> Example: Router(config-red)# interchassis group 230	Specifies that the port channel is an mLACP port channel. <ul style="list-style-type: none"> • The <i>group-id</i> should match the configured redundancy group.
Step 15	exit Example: Router(config-r-ic)# exit	Exits interchassis redundancy mode.
Step 16	exit Example: Router(config-red)# exit	Exits redundancy configuration mode.

	Command or Action	Purpose
Step 17	interface port-channel <i>port-channel- number</i> Example: Router(config)# interface port-channel1	Configures the port channel and enters interface configuration mode.
Step 18	service instance <i>id</i> ethernet [<i>evc-name</i>] Example: Router(config-if)# service instance 1 ethernet	Configures an Ethernet service instance and enters Ethernet service configuration mode.
Step 19	encapsulation dot1q <i>vlan-id</i> [, <i>vlan-id</i> [- <i>vlan-id</i>]] [native] Example: Router(config-if-srv)# encapsulation dot1q 100	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 20	exit Example: Router(config-if-srv)# exit	Exits service instance configuration mode.
Step 21	xconnect <i>peer-ip-address</i> <i>vc-id</i> { encapsulation mpls pw-class <i>pw-class-name</i> } [pw-class <i>pw-class-name</i>] [sequencing { transmit receive both }] Example: Router(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect	Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire.
Step 22	backup peer <i>peer-router-ip-addr</i> <i>vcid</i> [pw-class <i>pw-class-name</i>] [priority <i>value</i>] Example: Router(config-if)# backup peer 10.1.1.1 123 pw-class ether-pw	Specifies a redundant peer for a pseudowire virtual circuit.
Step 23	end Example: Router(config-if)# end	Returns the CLI to privileged EXEC mode.

Troubleshooting mLACP

Debugging mLACP

Use these **debug** commands for general mLACP troubleshooting.

SUMMARY STEPS

1. **enable**
2. **debug redundancy interchassis {all | application | error | event | monitor}**
3. **debug mpls ldp iccp**
4. **debug lacp [all | event| fsm| misc| multi-chassis [all | database | lacp-mgr | redundancy-group | user-interface] | packet]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug redundancy interchassis {all application error event monitor} Example: Router# debug redundancy interchassis all	<ul style="list-style-type: none"> • Enables debugging of the interchassis redundancy manager.
Step 3	debug mpls ldp iccp Example: Router# debug mpls ldp iccp	<ul style="list-style-type: none"> • Enables debugging of the InterChassis Control Protocol (ICCP).
Step 4	debug lacp [all event fsm misc multi-chassis [all database lacp-mgr redundancy-group user-interface] packet] Example: Router# debug lacp multi-chassis all	Enables debugging of LACP activity. <ul style="list-style-type: none"> • This command is run on the switch processor.

Debugging mLACP on an Attachment Circuit or EVC

Use these **debug** commands for troubleshooting mLACP on an attachment circuit or on an EVC.

SUMMARY STEPS

1. **enable**
2. **debug acircuit {checkpoint | error | event}**
3. **debug ethernet service {all | api | error | evc [evc-id] | ha | instance [id id | interface type number | qos] | interface type number | microblock | oam-mgr}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug acircuit {checkpoint error event} Example: Router# debug acircuit event	Displays checkpoints, errors, and events that occur on the attachment circuits between the PE and CE routers.
Step 3	debug ethernet service {all api error evc [evc-id] ha instance [id id interface type number qos] interface type number microblock oam-mgr} Example: Router# debug ethernet service all	Enables debugging of Ethernet customer service instances.

Debugging mLACP on AToM Pseudowires

Use the **debug mpls l2transport vc** command for troubleshooting mLACP on AToM pseudowires.

SUMMARY STEPS

1. **enable**
2. **debug mpls l2transport vc {event | fsm | ldp | sss | status {event | fsm}}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug mpls l2transport vc {event fsm ldp sss status {event fsm}} Example: Router# debug mpls l2transport status event	Displays information about the status of AToM virtual circuits (VCs).

Debugging Cross-Connect Redundancy Manager and Session Setup

Use the following **debug** commands to troubleshoot cross-connect, redundancy manager, and session setup.

SUMMARY STEPS

1. enable
2. debug sss error
3. debug sss events
4. debug xconnect {error | event}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug sss error Example: Router# debug sss error	Displays diagnostic information about errors that may occur during a subscriber service switch (SSS) call setup.

	Command or Action	Purpose
Step 3	debug sss events Example: Router# debug sss event	Displays diagnostic information about SSS call setup events.
Step 4	debug xconnect {error event} Example: Router# debug xconnect event	Displays errors or events related to a cross-connect configuration.

Debugging VFI

Use the **debug vfi** command for troubleshooting a VFI.

SUMMARY STEPS

1. **enable**
2. **debug vfi {checkpoint | error | event | fsm {error | event}}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug vfi {checkpoint error event fsm {error event}} Example: Router# debug vfi checkpoint	Displays checkpoint information about a VFI.

Debugging the Segment Switching Manager (Switching Setup)

Use the **debug ssm** command for troubleshooting a segment switching manager (SSM).

SUMMARY STEPS

1. enable
2. debug ssm {cm errors | cm events | fhm errors | fhm events | sm errors | sm events | sm counters | xdr}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug ssm {cm errors cm events fhm errors fhm events sm errors sm events sm counters xdr} Example: Router# debug ssm cm events	Displays diagnostic information about the SSM for switched Layer 2 segments.

Debugging High Availability Features in mLACP

Use the following **debug** commands for troubleshooting High Availability features in mLACP.

SUMMARY STEPS

1. enable
2. debug mpls l2transport checkpoint
3. debug acircuit checkpoint
4. debug vfi checkpoint

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

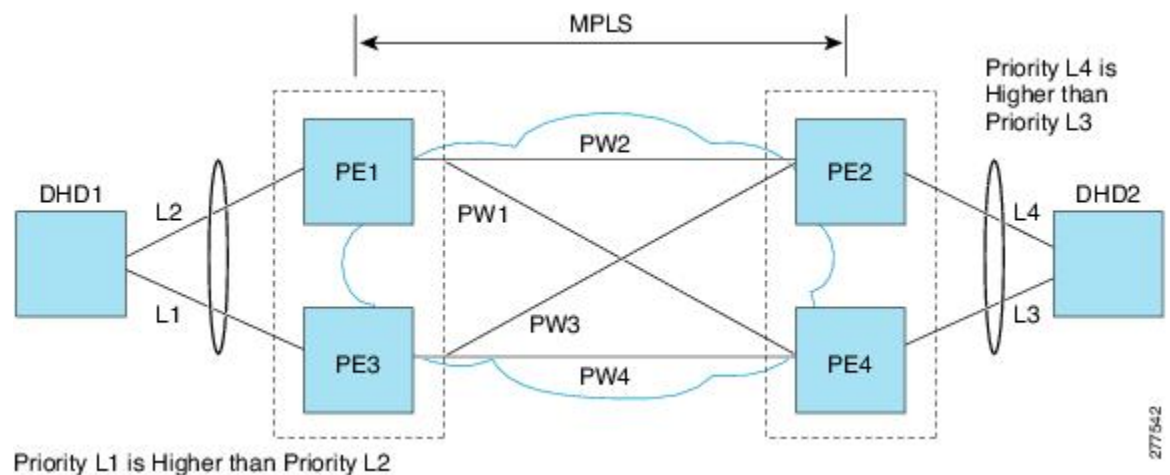
	Command or Action	Purpose
Step 2	debug mpls l2transport checkpoint Example: Router# debug mpls l2transport checkpoint	Enables the display of AToM events when AToM is configured for nonstop forwarding/stateful switchover (NSF/SSO) and Graceful Restart.
Step 3	debug acircuit checkpoint Example: Router# debug acircuit checkpoint	Enables the display of attachment circuit events when AToM is configured for NSF/SSO and Graceful Restart.
Step 4	debug vfi checkpoint Example: Router# debug vfi checkpoint	Enables the display of VFI events when AToM is configured for NSF/SSO and Graceful Restart.

Configuration Examples for mLACP

Example Configuring VPWS

Two sample configurations for VPWS follow: one example for an active PoA and the other for a standby PoA.

The figure below shows a sample topology for a VPWS configuration.



Active PoA for VPWS

The following VPWS sample configuration is for an active PoA:

```
mpls ldp graceful-restart
mpls label protocol ldp
!
redundancy
mode sso
interchassis group 1
member ip 201.0.0.1
backbone interface Ethernet0/2
backbone interface Ethernet1/2
backbone interface Ethernet1/3
monitor peer bfd
mlacp node-id 0
!
pseudowire-class mpls-dhd
encapsulation mpls
status peer topology dual-homed
!
interface Loopback0
ip address 200.0.0.1 255.255.255.255
!
interface Port-channel1
no ip address
lacp fast-switchover
lacp max-bundle 1
mlacp interchassis group 1
hold-queue 300 in
service instance 1 ethernet
encapsulation dot1q 100
xconnect 210.0.0.1 10 pw-class mpls-dhd
backup peer 211.0.0.1 10 pw-class mpls-dhd
!
interface Ethernet0/0
no ip address
channel-group 1 mode active
!
interface Ethernet1/3
ip address 10.0.0.200 255.255.255.0
mpls ip
bfd interval 50 min_rx 150 multiplier 3
```

Standby PoA for VPWS

The following VPWS sample configuration is for a standby PoA:

```
mpls ldp graceful-restart
mpls label protocol ldp
mpls ldp graceful-restart
mpls label protocol ldp
!
Redundancy
mode sso
interchassis group 1
member ip 200.0.0.1
backbone interface Ethernet0/2
backbone interface Ethernet1/2
backbone interface Ethernet1/3
monitor peer bfd
mlacp node-id 1
!
pseudowire-class mpls-dhd
encapsulation mpls
status peer topology dual-homed
!
```

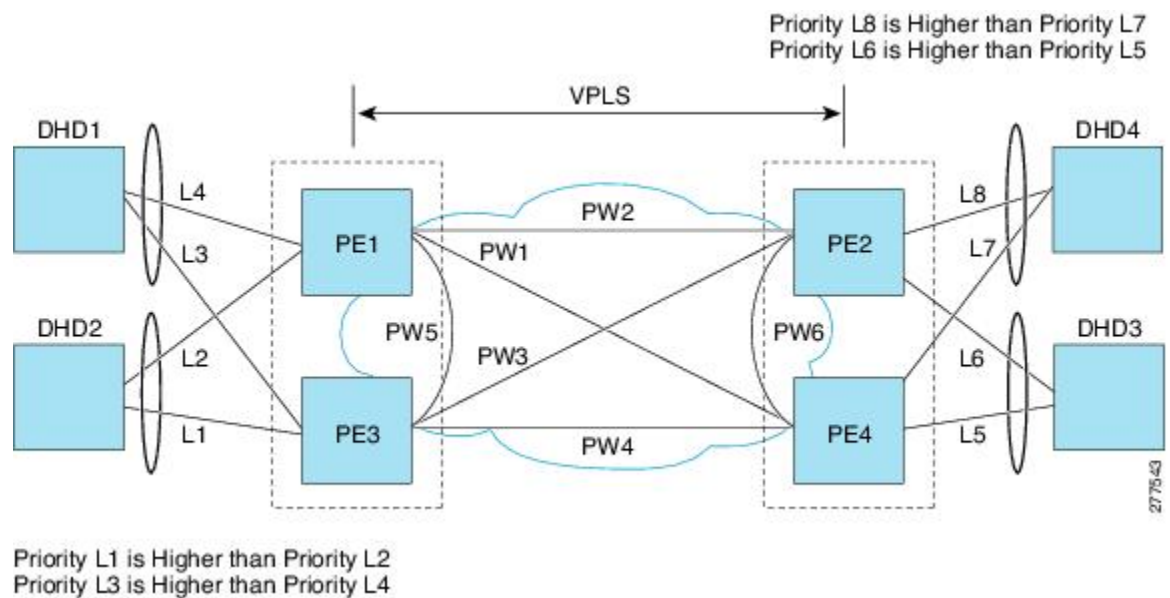
```

interface Loopback0
 ip address 201.0.0.1 255.255.255.255
!
interface Port-channel1
 no ip address
 lacp fast-switchover
 lacp max-bundle 1
 mlacp lag-priority 40000
 mlacp interchassis group 1
 hold-queue 300 in
 service instance 1 ethernet
 encapsulation dot1q 100
 xconnect 210.0.0.1 10 pw-class mpls-dhd
 backup peer 211.0.0.1 10 pw-class mpls-dhd
!
interface Ethernet1/0
 no ip address
 channel-group 1 mode active
!
interface Ethernet1/3
 ip address 10.0.0.201 255.255.255.0
 mpls ip
 bfd interval 50 min_rx 150 multiplier 3

```

Example Configuring VPLS

Two sample configurations for VPLS follow: one example for an active PoA and the other for a standby PoA. The figure below shows a sample topology for a VPLS configuration.



Active PoA for VPLS

The following VPLS sample configuration is for an active PoA:

```

mpls ldp graceful-restart
mpls label protocol ldp
!
redundancy

```

```

mode sso
interchassis group 1
member ip 201.0.0.1
backbone interface Ethernet0/2
monitor peer bfd
mlacp node-id 0
!
l2 vfi VPLS_200 manual
vpn id 10
neighbor 210.0.0.1 encapsulation mpls
neighbor 211.0.0.1 encapsulation mpls
neighbor 201.0.0.1 encapsulation mpls
!
interface Loopback0
ip address 200.0.0.1 255.255.255.255
!
interface Port-channel1
no ip address
lacp fast-switchover
lacp max-bundle 1
mlacp interchassis group 1
service instance 1 ethernet
encapsulation dot1q 100
bridge-domain 200
!
interface Ethernet0/0
no ip address
channel-group 1 mode active
!
interface Ethernet1/3
ip address 10.0.0.200 255.255.255.0
mpls ip
bfd interval 50 min_rx 150 multiplier 3
!
interface Vlan200
no ip address
xconnect vfi VPLS_200

```

Standby PoA for VPLS

The following VPLS sample configuration is for a standby PoA:

```

mpls ldp graceful-restart
mpls label protocol ldp
!
redundancy
interchassis group 1
member ip 200.0.0.1
backbone interface Ethernet0/2
monitor peer bfd
mlacp node-id 1
!
l2 vfi VPLS1 manual
vpn id 10
neighbor 210.0.0.1 encapsulation mpls
neighbor 211.0.0.1 encapsulation mpls
neighbor 200.0.0.1 encapsulation mpls
!
interface Loopback0
ip address 201.0.0.1 255.255.255.255
!
interface Port-channel1
no ip address
lacp fast-switchover
lacp max-bundle 1
mlacp lag-priority 40000
mlacp interchassis group 1
service instance 1 ethernet
encapsulation dot1q 100
bridge-domain 200

```



```

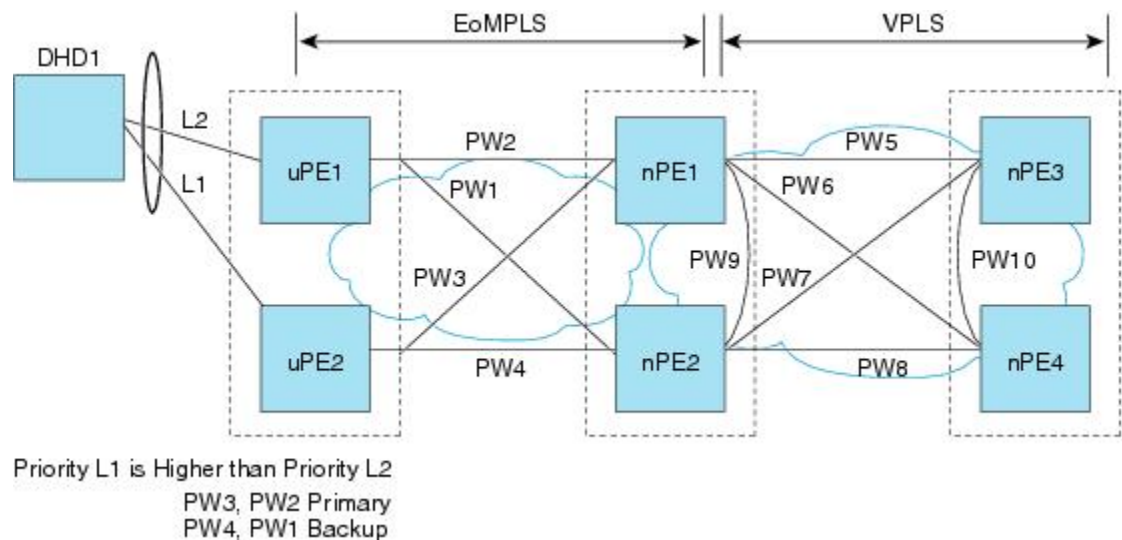
!
interface Ethernet1/0
 no ip address
 channel-group 1 mode active
!
interface Ethernet1/3
 ip address 10.0.0.201 255.255.255.0
 mpls ip
 bfd interval 50 min_rx 150 multiplier 3
!
interface Vlan200
 no ip address
 xconnect vfi VPLS_200

```

Example Configuring H-VPLS

Two sample configurations for H-VPLS follow: one example for an active PoA and the other for a standby PoA.

The figure below shows a sample topology for a H-VPLS configuration.



Active PoA for H-VPLS

The following H-VPLS sample configuration is for an active PoA:

```

mpls ldp graceful-restart
mpls label protocol ldp
!
redundancy
 mode sso
 interchassis group 1
  member ip 201.0.0.1
  backbone interface Ethernet0/2
  backbone interface Ethernet1/2
  backbone interface Ethernet1/3
  monitor peer bfd
  mlacp node-id 0
!
pseudowire-class mpls-dhd
 encapsulation mpls

```

```

    status peer topology dual-homed
  !
  interface Loopback0
  ip address 200.0.0.1 255.255.255.255
  !
  interface Port-channel1
  no ip address
  lacp fast-switchover
  lacp max-bundle 1
  mlacp interchassis group 1
  hold-queue 300 in
  service instance 1 ethernet
  encapsulation dot1q 100
  xconnect 210.0.0.1 10 pw-class mpls-dhd
  backup peer 211.0.0.1 10 pw-class mpls-dhd
  !
  interface Ethernet0/0
  no ip address
  channel-group 1 mode active
  !
  interface Ethernet1/3
  ip address 10.0.0.200 255.255.255.0
  mpls ip
  bfd interval 50 min_rx 150 multiplier 3

```

Standby PoA for H-VPLS

The following H-VPLS sample configuration is for a standby PoA:

```

mpls ldp graceful-restart
mpls label protocol ldp
!
Redundancy
mode sso
interchassis group 1
member ip 200.0.0.1
backbone interface Ethernet0/2
backbone interface Ethernet1/2
backbone interface Ethernet1/3
monitor peer bfd
mlacp node-id 1
!
pseudowire-class mpls-dhd
encapsulation mpls
status peer topology dual-homed
!
interface Loopback0
ip address 201.0.0.1 255.255.255.255
!
interface Port-channel1
no ip address
lacp fast-switchover
lacp max-bundle 1
mlacp lag-priority 40000
mlacp interchassis group 1
hold-queue 300 in
service instance 1 ethernet
encapsulation dot1q 100
xconnect 210.0.0.1 10 pw-class mpls-dhd
backup peer 211.0.0.1 10 pw-class mpls-dhd
!
interface Ethernet1/0
no ip address
channel-group 1 mode active
!
interface Ethernet1/3
ip address 10.0.0.201 255.255.255.0
mpls ip
bfd interval 50 min_rx 150 multiplier 3

```

Example Verifying VPWS on an Active PoA

The following **show** commands can be used to display statistics and configuration parameters to verify the operation of the mLACP feature on an active PoA:

show lacp multichassis group

Use the **show lacp multichassis group** command to display the interchassis redundancy group value and the operational LACP parameters.

```
Router# show lacp multichassis group 100
Interchassis Redundancy Group 100
Operational LACP Parameters:
RG State:      Synchronized
System-Id:    200.000a.f331.2680
ICCP Version: 0
Backbone Uplink Status: Connected
Local Configuration:
Node-id:      0
System-Id:    200.000a.f331.2680
Peer Information:
State:        Up
Node-id:      7
System-Id:    2000.0014.6a8b.c680
ICCP Version: 0
State Flags:  Active      - A
               Standby    - S
               Down       - D
               AdminDown  - AD
               Standby Reverting - SR
               Unknown    - U

mLACP Channel-groups
Channel  State      Priority      Active Links      Inactive Links
Group   Local/Peer  Local/Peer    Local/Peer        Local/Peer
1       A/S        28000/32768   4/4               0/0
```

show lacp multichassis port-channel

Use the **show lacp multichassis port-channel** command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

```
Router# show lacp multichassis port-channel1
Interface Port-channel1
Local Configuration:
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
                  Bundled: 4
                  Selected: 4
                  Standby: 0
                  Unselected: 0
Peer Configuration:
Interface: Port-channel1
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
```

```

Priority: 32768
Inactive Links: 0
Total Active Links: 4
                        Bundled: 0
                        Selected: 0
                        Standby: 4
                        Unselected: 0

```

show mpls ldp iccp

Use the **show mpls ldp iccp** command to display the LDP session and ICCP state information.

```

Router# show mpls ldp iccp

ICPM RGID Table
iccp:
  rg_id: 100, peer addr: 172.3.3.3
  ldp_session 0x3, client_id 0
  iccp state: ICPM_ICCP_CONNECTED
  app type: MLACP
  app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
iccp:
  rg_id: 100, peer addr: 172.3.3.3
  ldp_session 0x3, client_id 0
  iccp state: ICPM_ICCP_CONNECTED
  app type: MLACP
  app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

```

show mpls l2transport

Use the **show mpls l2transport** command to display the local interface and session details, destination address, and status.

```

Router# show mpls l2transport vc 2
-----
Local intf    Local circuit    Dest address    VC ID    Status
-----
Po1           Eth VLAN 2       172.2.2.2       2        UP
Po1           Eth VLAN 2       172.4.4.4       2        STANDBY

```

show etherchannel summary

Use the **show etherchannel summary** command to display the status and identity of the mLACP member links.

```

Router# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 2
Number of aggregators:          2
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(RU)        LACP        Gi2/9(P)   Gi2/20(P)  Gi2/31(P)

```

show etherchannel number port-channel

Use the **show etherchannel number port-channel** command to display the status and identity of the EtherChannel and port channel.

```
Router# show etherchannel 51 port-c

Port-channels in the group:
-----

Port-channel: Po51      (Primary Aggregator)

-----

Age of the Port-channel   = 0d:02h:25m:23s
Logical slot/port        = 14/11          Number of ports = 2
HotStandBy port = null
Passive port list        = Gi9/15 Gi9/16
Port state                = Port-channel L3-Ag Ag-Inuse
Protocol                  = LACP
Fast-switchover          = enabled
Direct Load Swap         = disabled

Ports in the Port-channel:

Index  Load   Port      EC state      No of bits
-----+-----+-----+-----+-----
  0     55    Gi9/15    mLACP-stdby   4
  1     AA    Gi9/16    mLACP-stdby   4

Time since last port bundled:    0d:01h:03m:39s    Gi9/16
Time since last port Un-bundled: 0d:01h:03m:40s    Gi9/16

Last applied Hash Distribution Algorithm: Fixed Channel-group Iedge Counts:
-----:
Access ref count                : 0
Iedge session count             : 0
```

show lacp internal

Use the **show lacp internal** command to display the device, port, and member- link information.

```
Router# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags   State   LACP port   Admin   Oper   Port      Port
Gi2/9     SA      bndl-act 28000       0x1     0x1     0x820A    0x3D
Gi2/20    SA      bndl-act 28000       0x1     0x1     0x8215    0x3D
Gi2/31    SA      bndl-act 28000       0x1     0x1     0x8220    0x3D
Gi2/40    SA      bndl-act 28000       0x1     0x1     0x8229    0x3D
Peer (MLACP-PE3) mLACP member links
Gi3/11    FA      hot-sby  32768       0x1     0x1     0xF30C    0x5
Gi3/21    FA      hot-sby  32768       0x1     0x1     0xF316    0x5
Gi3/32    FA      hot-sby  32768       0x1     0x1     0xF321    0x7
Gi3/2     FA      hot-sby  32768       0x1     0x1     0xF303    0x7
```

Example Verifying VPWS on a Standby PoA

The following **show** commands can be used to display statistics and configuration parameters to verify the operation of the mLACP feature on a standby PoA:

show lacp multichassis group

Use the **show lacp multichassis group** command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, node ID, channel, state, priority active, and inactive links.

```
Router# show lacp multichassis group 100
Interchassis Redundancy Group 100
Operational LACP Parameters:
RG State:      Synchronized
System-Id:     200.000a.f331.2680
ICCP Version:  0
Backbone Uplink Status: Connected
Local Configuration:
Node-id:       7
System-Id:     2000.0014.6a8b.c680
Peer Information:
State:         Up
Node-id:       0
System-Id:     200.000a.f331.2680
ICCP Version:  0
State Flags:   Active      - A
               Standby    - S
               Down       - D
               AdminDown   - AD
               Standby Reverting - SR
               Unknown     - U

mLACP Channel-groups
Channel      State      Priority      Active Links      Inactive Links
Group      Local/Peer  Local/Peer    Local/Peer        Local/Peer
1          S/A        32768/28000   4/4               0/0
```

show lacp multichassis portchannel

Use the **show lacp multichassis portchannel** command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

```
Router# show lacp multichassis port-channel1
Interface Port-channel1
Local Configuration:
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
                Bundled: 0
                Selected: 0
                Standby: 4
                Unselected: 0
Peer Configuration:
Interface: Port-channel1
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
                Bundled: 4
                Selected: 4
                Standby: 0
                Unselected: 0
```

show mpls ldp iccp

Use the **show mpls ldp iccp** command to display the LDP session and ICCP state information.

```
Router# show mpls ldp iccp
ICPM RGID Table
  iccp:
    rg_id: 100, peer addr: 172.1.1.1
    ldp_session 0x2, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
  iccp:
    rg_id: 100, peer addr: 172.1.1.1
    ldp_session 0x2, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1
```

show mpls l2transport

Use the **show mpls l2transport** command to display the local interface and session details, destination address, and status.

```
Router# show mpls l2transport vc 2
```

Local intf	Local circuit	Dest address	VC ID	Status
Pol	Eth VLAN 2	172.2.2.2	2	STANDBY
Pol	Eth VLAN 2	172.4.4.4	2	STANDBY

show etherchannel summary

Use the **show etherchannel summary** command to display the status and identity of the mLACP member links.

```
Router# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone   S - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
Number of channel-groups in use: 2
Number of aggregators:          2
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
```

1	Pol (RU)	LACP	Gi3/2 (P) Gi3/32 (P)	Gi3/11 (P)	Gi3/21 (P)
---	----------	------	-------------------------	------------	------------

show lacp internal

Use the **show lacp internal** command to display the device, port, and member-link information.

```
Router# show lacp 1 internal
```

```

Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode
Channel group 1

Port      Flags   State      LACP port  Admin   Oper   Port      Port
Gi3/2     FA       bndl-sby  32768      0x1     0x1    0xF303    0x7
Gi3/11    FA       bndl-sby  32768      0x1     0x1    0xF30C    0x5
Gi3/21    FA       bndl-sby  32768      0x1     0x1    0xF316    0x5
Gi3/32    FA       bndl-sby  32768      0x1     0x1    0xF321    0x7
Peer (MLACP-PE1) mLACP member links
Gi2/20    SA       bndl      28000      0x1     0x1    0x8215    0x3D
Gi2/31    SA       bndl      28000      0x1     0x1    0x8220    0x3D
Gi2/40    SA       bndl      28000      0x1     0x1    0x8229    0x3D
Gi2/9     SA       bndl      28000      0x1     0x1    0x820A    0x3D

```

Example Verifying VPLS on an Active PoA

The following **show** commands can be used to display statistics and configuration parameters to verify the operation of the mLACP feature on an active PoA:

show lacp multichassis group

Use the **show lacp multichassis group** command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, node ID, channel, state, priority active, and inactive links.

```

Router# show lacp multichassis group 100
Interchassis Redundancy Group 100
Operational LACP Parameters:
RG State:      Synchronized
System-Id:     200.000a.f331.2680
ICCP Version:  0
Backbone Uplink Status: Connected
Local Configuration:
Node-id:       0
System-Id:     200.000a.f331.2680
Peer Information:
State:         Up
Node-id:       7
System-Id:     2000.0014.6a8b.c680
ICCP Version:  0
State Flags:   Active      - A
               Standby     - S
               Down        - D
               AdminDown   - AD
               Standby Reverting - SR
               Unknown     - U

mLACP Channel-groups
Channel  State      Priority   Active Links   Inactive Links
Group   Local/Peer  Local/Peer Local/Peer      Local/Peer
1       A/S        28000/32768 4/4            0/0

```

show lacp multichassis port-channel

Use the **show lacp multichassis port-channel** command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

```

Router# show lacp multichassis port-channel1
Interface Port-channel1
Local Configuration:
Address: 000a.f331.2680

```



```

Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
    Bundled: 4
    Selected: 4
    Standby: 0
    Unselected: 0
Peer Configuration:
Interface: Port-channel1
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
    Bundled: 0
    Selected: 0
    Standby: 4
    Unselected: 0

```

show mpls ldp iccp

Use the **show mpls ldp iccp** command to display the LDP session and ICCP state information.

```

Router# show mpls ldp iccp
ICPM RGID Table
  iccp:
    rg_id: 100, peer addr: 172.3.3.3
    ldp_session 0x3, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
  iccp:
    rg_id: 100, peer addr: 172.3.3.3
    ldp_session 0x3, client_id 0
    iccp state: ICPM_ICCP_CONNECTED
    app type: MLACP
    app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

```

show mpls l2transport

Use the **show mpls l2transport** command to display the local interface and session details, destination address, and the status.

```

Router# show mpls l2transport vc 4000

```

Local intf	Local circuit	Dest address	VC ID	Status
VFI VPLS	VFI	172.2.2.2	4000	UP
VFI VPLS	VFI	172.4.4.4	4000	UP

show etherchannel summary

Use the **show etherchannel summary** command to display the status and identity of the mLACP member links.

```

Router# show etherchannel summary

```

Example Verifying VPLS on a Standby PoA

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 2
Number of aggregators:          2
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1       Po1 (RU)          LACP        Gi2/9 (P)   Gi2/20 (P)   Gi2/31 (P)
                               Gi2/40 (P)

```

show lacp internal

Use the **show lacp internal** command to display the device, port, and member-link information.

```

Router# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode          P - Device is in Passive mode
Channel group 1

Port      Flags   State      LACP port   Admin   Oper   Port      Port
Gi2/9     SA       bndl-act   28000       0x1     0x1    0x820A    0x3D
Gi2/20    SA       bndl-act   28000       0x1     0x1    0x8215    0x3D
Gi2/31    SA       bndl-act   28000       0x1     0x1    0x8220    0x3D
Gi2/40    SA       bndl-act   28000       0x1     0x1    0x8229    0x3D
Peer (MLACP-PE3) mLACP member links
Gi3/11    FA       hot-sby    32768       0x1     0x1    0xF30C    0x5
Gi3/21    FA       hot-sby    32768       0x1     0x1    0xF316    0x5
Gi3/32    FA       hot-sby    32768       0x1     0x1    0xF321    0x7
Gi3/2     FA       hot-sby    32768       0x1     0x1    0xF303    0x7

```

Example Verifying VPLS on a Standby PoA

The **show** commands in this section can be used to display statistics and configuration parameters to verify the operation of the mLACP feature:

show lacp multichassis group

Use the **show lacp multichassis group *interchassis group number*** command to display the LACP parameters, local configuration, status of the backbone uplink, peer information, node ID, channel, state, priority, active, and inactive links.

```

Router# show lacp multichassis group 100
Interchassis Redundancy Group 100
Operational LACP Parameters:
RG State:      Synchronized
System-Id:     200.000a.f331.2680
ICCP Version:  0
Backbone Uplink Status: Connected
Local Configuration:
Node-id:       7
System-Id:     2000.0014.6a8b.c680
Peer Information:
State:         Up
Node-id:       0
System-Id:     200.000a.f331.2680

```

```

ICCP Version: 0
State Flags: Active      - A
               Standby   - S
               Down      - D
               AdminDown - AD
               Standby Reverting - SR
               Unknown    - U

mLACP Channel-groups
Channel  State      Priority      Active Links      Inactive Links
Group   Local/Peer   Local/Peer   Local/Peer        Local/Peer
  1      S/A        32768/28000   4/4                0/0

```

show lacp multichassis portchannel

Use the **show lacp multichassis portchannel** command to display the interface port-channel value channel group, LAG state, priority, inactive links peer configuration, and standby links.

```

Router# show lacp multichassis port-channel1
Interface Port-channel1
Local Configuration:
Address: 0014.6a8b.c680
Channel Group: 1
State: Standby
LAG State: Up
Priority: 32768
Inactive Links: 0
Total Active Links: 4
                Bundled: 0
                Selected: 0
                Standby: 4
                Unselected: 0
Peer Configuration:
Interface: Port-channel1
Address: 000a.f331.2680
Channel Group: 1
State: Active
LAG State: Up
Priority: 28000
Inactive Links: 0
Total Active Links: 4
                Bundled: 4
                Selected: 4
                Standby: 0
                Unselected: 0

```

show mpls ldp iccp

Use the **show mpls ldp iccp** command to display the LDP session and ICCP state information.

```

Router# show mpls ldp iccp
ICPM RGID Table
iccp:
  rg_id: 100, peer addr: 172.1.1.1
  ldp_session 0x2, client_id 0
  iccp state: ICPM_ICCP_CONNECTED
  app type: MLACP
  app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM RGID Table total ICCP sessions: 1
ICPM LDP Session Table
iccp:
  rg_id: 100, peer addr: 172.1.1.1
  ldp_session 0x2, client_id 0
  iccp state: ICPM_ICCP_CONNECTED
  app type: MLACP

```

```

app state: ICPM_APP_CONNECTED, ptcl ver: 0
ICPM LDP Session Table total ICCP sessions: 1

```

show mpls l2transport vc 2

Use the **show mpls l2transport** command to display the local interface and session details, destination address, and status.

```

Router# show mpls l2transport vc 2
-----
Local intf   Local circuit   Dest address   VC ID   Status
-----
VFI VPLS     VFI             172.2.2.2     4000     UP
VFI VPLS     VFI             172.4.4.4     4000     UP

```

show etherchannel summary

Use the **show etherchannel summary** command to display the status and identity of the mLACP member links.

```

Router# show etherchannel summary

Flags: D - down          P - bundled in port-channel
       I - stand-alone   s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2
-----
Group  Port-channel  Protocol    Ports
-----
1      Po1(RU)         LACP        Gi3/2(P)  Gi3/11(P)  Gi3/21(P)
                        Gi3/32(P)

```

show lacp internal

Use the **show lacp internal** command to display the device, port, and member- link information.

```

Router# show lacp 1 internal

Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode          P - Device is in Passive mode

Channel group 1

Port      Flags   State    LACP port   Admin   Oper   Port      Port
Gi3/2     FA      bndl-sby 32768       0x1     0x1     0xF303    0x7
Gi3/11    FA      bndl-sby 32768       0x1     0x1     0xF30C    0x5
Gi3/21    FA      bndl-sby 32768       0x1     0x1     0xF316    0x5
Gi3/32    FA      bndl-sby 32768       0x1     0x1     0xF321    0x7
Peer (MLACP-PE1) mLACP member links
Gi2/20    SA      bndl     28000       0x1     0x1     0x8215    0x3D
Gi2/31    SA      bndl     28000       0x1     0x1     0x8220    0x3D
Gi2/40    SA      bndl     28000       0x1     0x1     0x8229    0x3D
Gi2/9     SA      bndl     28000       0x1     0x1     0x820A    0x3D

```

Glossary

active attachment circuit—The link that is actively forwarding traffic between the DHD and the active PoA.

active PW—The pseudowire that is forwarding traffic on the active PoA.

BD—bridge domain.

BFD—bidirectional forwarding detection.

DHD—dual-homed device. A node that is connected to two switches over a multichassis link aggregation group for the purpose of redundancy.

DHN—dual-homed network. A network that is connected to two switches to provide redundancy.

H-VPLS—Hierarchical Virtual Private LAN Service.

ICC—Interchassis Communication Channel.

ICCP—Interchassis Communication Protocol.

ICPM—Interchassis Protocol Manager.

ICRM—Interchassis Redundancy Manager.

LACP—Link Aggregation Control Protocol.

LAG—link aggregation group.

LDP—Link Distribution Protocol.

MCEC—Multichassis EtherChannel.

mLACP—Multichassis LACP.

PoA—point of attachment. One of a pair of switches running multichassis link aggregation group with a DHD.

PW-RED—pseudowire redundancy.

standby attachment circuit—The link that is in standby mode between the DHD and the standby PoA.

standby PW—The pseudowire that is in standby mode on either an active or a standby PoA.

uPE—user-facing Provider Edge.

VPLS—Virtual Private LAN Service.

VPWS—Virtual Private Wire Service.

