Application Services Configuration Guide, Cisco IOS XE 17.x

First Published: 2022-11-05

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

CONTENTS

Full Cisco Trademarks with Software License

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.

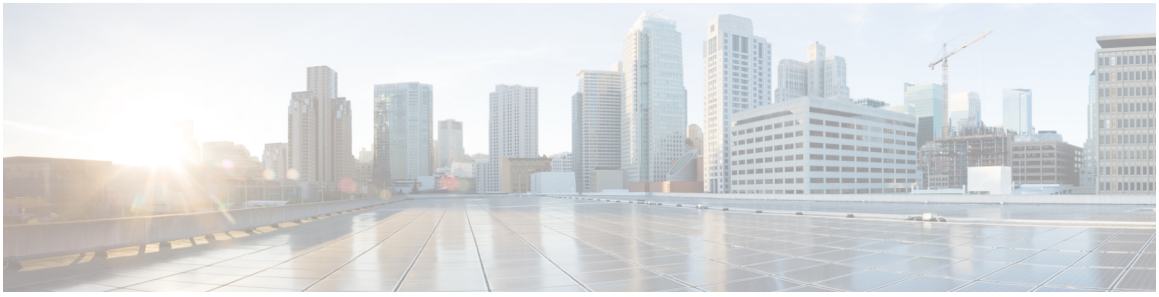
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)



Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:

Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the Cisco Feature Navigator tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

Document Conventions

This documentation uses the following conventions:

Convention	Description
^ or **Ctrl**	The ^ and **Ctrl** symbols represent the Control key. For example, the key combination **^D** or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Keys are indicated in capital letters but are not case sensitive.
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

The command syntax descriptions use the following conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter exactly as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`bold screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

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

Note Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

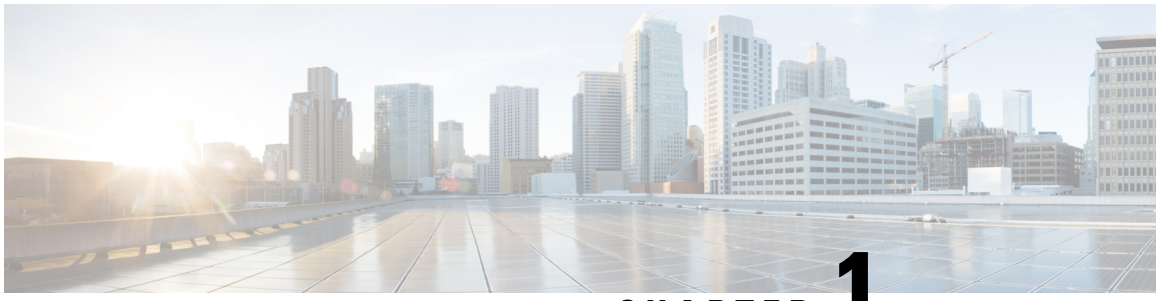
Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

PART I

ATM



CHAPTER 1

Configuring ATM

This chapter describes how to configure ATM on the Cisco ASR 1000 Series Aggregation Services Routers.

Restrictions for Configuring ATM

Restrictions for PVC Bundle Management

ATM PVC Bundling Support on ASR1K

- A maximum of 8 PVCs can be configured in one PVC bundle.

ATM Interface

Asynchronous Transfer Mode (ATM) uses one Virtual Circuit (VC) to carry all traffic to the next hop address. Even with VC multiplexing, a single VC carries all traffic of the same protocol to the next hop address. Though Weighted Random Early Discard (Per-VC (D)WRED) and WFQ can classify and prioritize the packets, they all share one single Quality of Service (QoS) VC.

Enabling the ATM Interface

This section describes how to configure an ATM interface. For the AIP, all ATM port adapters, and the 1-port ATM-25 network module, the port number is always 0. For example, the *slot*/*port* address of an ATM interface on an AIP installed in slot 1 is 1/0.

To configure the ATM interface, use the following commands beginning in privileged EXEC mode:

SUMMARY STEPS

1. Device# **configure terminal**
2. Do one of the following:
   - Device(config)# **interface atm** *slot* **/0**
   - Device(config)# **interface atm** *slot* **/** *port-adapter* **/0**
3. Device(config-if)# **ip address** *ip-address mask*
4. Device(config-if)# **no shutdown**

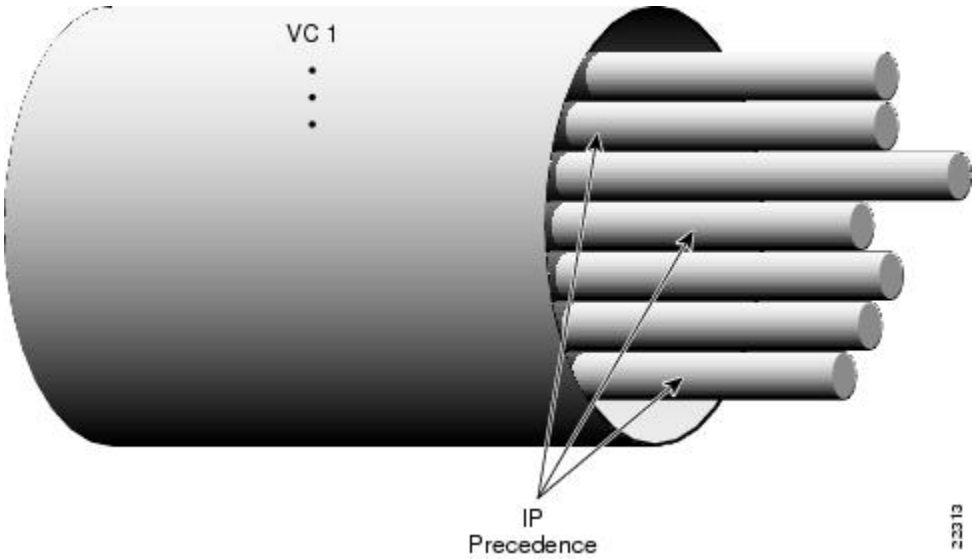
DETAILED STEPS

	Command or Action	Purpose
Step 1	Device# **configure terminal**	Enters global configuration mode from the terminal.
Step 2	Do one of the following: • Device(config)# **interface atm** *slot* **/0** • Device(config)# **interface atm** *slot* **/** *port-adapter* **/0** **Example:** `Device(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command. To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or device documentation.
Step 3	Device(config-if)# **ip address** *ip-address mask*	(Optional) If IP routing is enabled on the system, assigns a source IP address and subnet mask to the interface.
Step 4	Device(config-if)# **no shutdown**	Changes the shutdown state to up and enables the ATM interface, thereby beginning the segmentation and reassembly (SAR) operation on the interface. • The **no shutdown** command passes an **enable** command to the ATM interface, which then begins segmentation and reassembly (SAR) operations. It also causes the ATM interface to configure itself based on the previous configuration commands sent.

VC Bundle Support and Bundle Management

ATM VC bundle management allows you to configure multiple VCs that have different QoS characteristics between any pair of ATM-connected routers. As shown in the figure below, these VCs are grouped in a bundle and are referred to as bundle members.

Figure 1: ATM VC Bundle

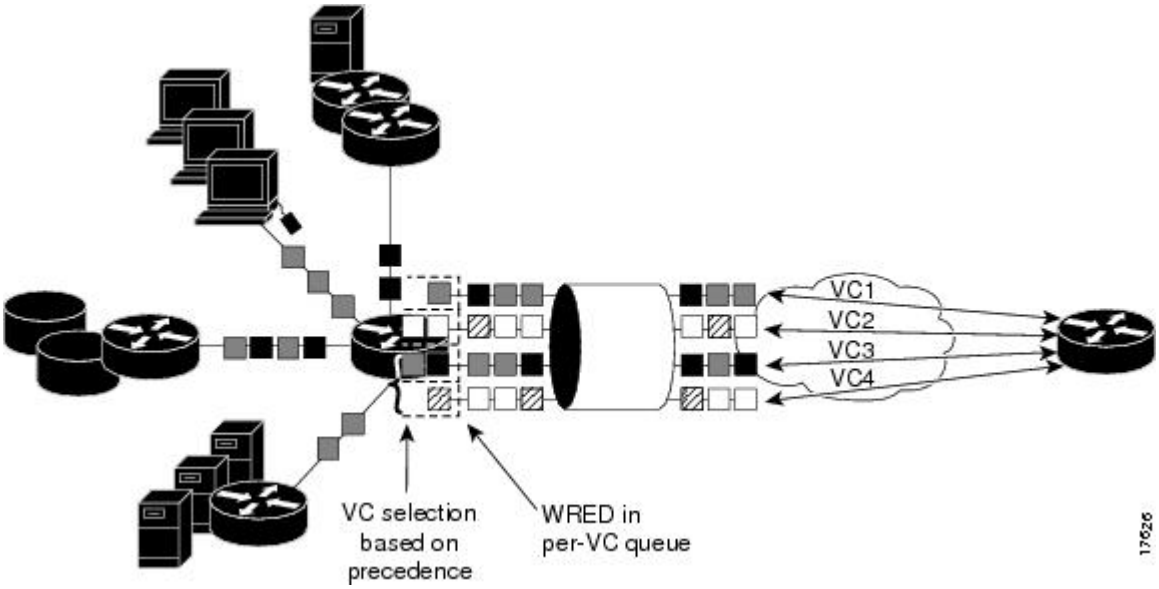


ATM VC bundle management allows you to define an ATM VC bundle and add VCs to it. Each VC of a bundle has its own ATM traffic class and ATM traffic parameters. You can apply attributes and characteristics to discrete VC bundle members or you can apply them collectively at the bundle level.

Using VC bundles, you can create differentiated service by flexibly distributing IP precedence levels over the different VC bundle members. You can map a single precedence level or a range of levels to each discrete VC in the bundle, thereby enabling individual VCs in the bundle to carry packets marked with different precedence levels. You can use WRED (or DWRED) to further differentiate service across traffic that has different IP precedences but that uses the same VC in a bundle.

To determine which VC in the bundle to use to forward a packet to its destination, the ATM VC bundle management software matches precedence levels between packets and VCs (see the figure below). IP traffic is sent to the next hop address for the bundle because all VCs in a bundle share the same destination, but the VC used to carry a packet depends on the value set for that packet in the IP Precedence bits of the type of service (ToS) byte of its header. The ATM VC bundle management software matches the IP precedence of the packet to the IP Precedence value or range of values assigned to a VC, sending the packet out on the appropriate VC. Moreover, the ATM VC bundle management feature allows you to configure how traffic will be redirected when the VC the packet was matched to goes down. The figure below illustrates how the ATM VC bundle management software determines which permanent virtual circuit (PVC) bundle member to use to carry a packet and how WRED (or DWRED) is used to differentiate traffic on the same VC.

Figure 2: ATM VC Bundle PVC Selection for Packet Transfer



The support of multiple parallel ATM VCs allows you to create stronger service differentiation at the IP layer. For instance, you might want to provide IP traffic belonging to real-time CoS (such as Voice over IP traffic) on an ATM VC with strict constraints (constant bit rate (CBR) or variable bit rate real-time (VBR-rt), for example), while transporting traffic other than real-time traffic over a more elastic ATM available bit rate (ABR) PVC. Using a configuration such as this would allow you to fully utilize your network capacity. You could also elect to transport best-effort IP traffic over an unspecified bit rate (UBR) PVC--UBR is effectively the ATM version of best-effort service.

How to Configure ATM

To configure ATM, complete the tasks in the following sections. The first task is required, and then you must configure at least one PVC or SVC. The virtual circuit options you configure must match in three places: on the router, on the ATM switch, and at the remote end of the PVC or SVC connection. The remaining tasks are optional.

Configuring a VC Bundle

Creating a VC Bundle

Command	Purpose
`Device(config-if)# bundle bundle-name`	Creates the specified bundle and enters bundle configuration mode.

Applying Parameters to Individual VCs

Configuring a VC Bundle Member Directly

Command	Purpose
`Device(config-if-atm-member)# ubr output-pcr [input-pcr]`	Configures the VC for unspecified bit rate (UBR) QoS and specifies the output peak cell rate (PCR) for it.
`Device(config-if-atm-member)# ubr+ output-pcr output-mcr [input-pcr] [input-mcr]`	Configures the VC for UBR QoS and specifies the output PCR and output minimum guaranteed cell rate for it.
`Device(config-if-atm-member)# vbr-nrt output-pcr output-scr output-mbs [input-pcr] [input-scr] [input-mbs]`	Configures the VC for variable bit rate nonreal-time (VBR-nrt) QoS and specifies the output PCR, output sustainable cell rate, and output maximum burst cell size for it.
`Device(config-if-atm-member)# precedence [other | range]`	Configures the precedence levels for the VC.
`Device(config-if-atm-member)# bump {implicit | explicit precedence-level | traffic}`	Configures the bumping rules for the VC.
`Device(config-if-atm-member)# protect {group | vc}`	Configures the VC to belong to the protected group of the bundle or to be an individually protected VC bundle member.

Configuring VC Class Parameters to Apply to a VC Bundle Member

Command	Purpose
`Device(config-vc-class)# bump {implicit | explicit precedence-level | traffic}`	Specifies the bumping rules for the VC member to which the class is applied. These rules determine to which VC in the bundle traffic is directed when the carrier VC bundle member goes down. **Note** You can also add the following commands to a VC class to be used to configure a VC bundle member: **ubr**, **ubr+**, and **vbr-nrt**. When a VC is a member of a VC bundle, the following commands cannot be used in vc-class mode to configure the VC: **encapsulation**, **protocol**, **inarp**, and **broadcast**. These commands are useful only at the bundle level, not the bundle member level. Configuration for an individual VC overrides the collective configuration applied to all VC bundle members through application of a VC class to the bundle.

Command	Purpose
`Device(config-vc-class)# precedence precedence min-threshold max-threshold mark-probability-denominator`	Defines precedence levels for the VC member to which the class is applied.
`Device(config-vc-class)# protect {group | vc}`	Configures the VC as a member of the protected group of the bundle or as an individually protected VC.

Applying a VC Class to a Discrete VC Bundle Member

Command	Purpose
`Device(config-if-atm-member)# class-vc vc-class-name`	Assigns a VC class to a VC bundle member.

Configuring a VC Not to Accept Bumped Traffic

Command	Purpose
`Device(config-if-atm-member)# no bump traffic`	Configures the VC not to accept any bumped traffic that would otherwise be redirected to it.

Monitoring and Maintaining VC Bundles and Their VC Members

Command	Purpose
`Device# show atm bundle bundle-name`	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
`Device# show atm bundle bundle-name statistics [detail]`	Displays statistics or detailed statistics on the specified bundle.
`Device# show atm map`	Displays a list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.
`Device# debug atm bundle errors`	Displays information on bundle errors.
`Device# debug atm bundle events`	Displays a record of bundle events.

Applying Bundle-Level Parameters

Configuring Bundle-Level Parameters

Command	Purpose
`Device(config-atm-bundle)# protocol protocol {protocol-address | inarp} [[no] broadcast]`	Configures a static map or enables Inverse Address Resolution Protocol (Inverse ARP) or Inverse ARP broadcasts for the bundle. **Note** Bundle-level parameters can be applied either by assigning VC classes or by directly applying them to the bundle. Parameters applied through a VC class assigned to the bundle are superseded by those applied at the bundle level. Bundle-level parameters are superseded by parameters applied to an individual VC.
`Device(config-atm-bundle)# encapsulation aal-encap`	Configures the ATM adaptation layer (AAL) and encapsulation type for the bundle.
`Device(config-atm-bundle)# inarp minutes`	Configures the Inverse ARP time period for all VC bundle members.
`Device(config-atm-bundle)# broadcast`	Enables broadcast forwarding for all VC bundle members.
`Device(config-atm-bundle)# oam retry up-count down-count retry frequency`	Configures the VC bundle parameters related to operation, administration, and maintenance (OAM) management.
`Device(config-atm-bundle)# oam-bundle [manage] [frequency]`	Enables end-to-end F5 OAM loopback cell generation and OAM management for all VCs in the bundle.

Configuring VC Class Parameters to Apply to a VC Bundle Member

Command	Purpose
`Device(config-vc-class)# bump {implicit | explicit precedence-level | traffic}`	Specifies the bumping rules for the VC member to which the class is applied. These rules determine to which VC in the bundle traffic is directed when the carrier VC bundle member goes down. **Note** You can also add the following commands to a VC class to be used to configure a VC bundle member: **ubr**, **ubr+**, and **vbr-nrt**. When a VC is a member of a VC bundle, the following commands cannot be used in vc-class mode to configure the VC: **encapsulation**, **protocol**, **inarp**, and **broadcast**. These commands are useful only at the bundle level, not the bundle member level. Configuration for an individual VC overrides the collective configuration applied to all VC bundle members through application of a VC class to the bundle.

Command	Purpose
`Device(config-vc-class)# precedence precedence min-threshold max-threshold mark-probability-denominator`	Defines precedence levels for the VC member to which the class is applied.
`Device(config-vc-class)# protect {group | vc}`	Configures the VC as a member of the protected group of the bundle or as an individually protected VC.

Attaching a Class to a Bundle

Command	Purpose
`(config-atm-bundle)# class-bundle vc-class-name`	Configures a bundle with the bundle-level commands contained in the specified VC class. **Note** Parameters set through bundle-level commands contained in the VC class are applied to the bundle and all of its VC members. Bundle-level parameters applied through commands configured directly on the bundle supersede those applied through a VC class. Some bundle-level parameters applied through a VC class or directly to the bundle can be superseded by commands that you directly apply to individual VCs in bundle-vc configuration mode.

Committing a VC to a Bundle

Command	Purpose
`Device(config-atm-bundle)# pvc-bundle pvc-name [vpi/] [vci]`	Adds the specified VC to the bundle and enters bundle-vc configuration mode in order to configure the specified VC bundle member.

Configuring PVCs

To use a permanent virtual circuit (PVC), you must configure the PVC into both the router and the ATM switch. PVCs remain active until the circuit is removed from either configuration.

When a PVC is configured, all the configuration options are passed on to the ATM interface. These PVCs are writable into the nonvolatile RAM (NVRAM) as part of the Route Processor (RP) configuration and are used when the RP image is reloaded.

Some ATM switches might have point-to-multipoint PVCs that do the equivalent of broadcasting. If a point-to-multipoint PVC exists, then that PVC can be used as the sole broadcast PVC for all multicast requests.

To configure a PVC, perform the tasks in the following sections.

Creating a Permanent Virtual Circuit

To use a permanent virtual circuit (PVC), configure the PVC in both the router and the ATM switch. PVCs remain active until the circuit is removed from either configuration. To create a PVC on the ATM interface

and enter interface ATM VC configuration mode, perform the following procedure beginning in global configuration mode:

SUMMARY STEPS

1. Device(config)# **interface atm** *slot*/*subslot*/*port***.***subinterface* [**.***subinterface-number* {**multipoint** | **point-to-point**}]
2. (config-if)# **ipaddress***address mask*
3. Device(config-if)# **pvc** [*name*] *vpi* /*vci*
4. Device(config-if-atm-vc)# **protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**]
5. Device(config-if-atm-vc)# **inarp** *minutes*
6. Device(config-if-atm-vc)# **encapsulation** {**aal5mux**|**aal5nlpidaal5snap**}
7. Device(config-if-atm-vc)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **interface atm** *slot*/*subslot*/*port***.***subinterface* [**.***subinterface-number* {**multipoint**	**point-to-point**}]	Enters subinterface configuration mode for the specified port on the ATM Interface Module (IM), where: • *slot*—Specifies the chassis slot number where the SIP is installed. • *subslot*—Specifies the secondary slot of the SIP where the IM is installed. • *port*—Specifies the number of the individual interface port on an IM. • *subinterface*—Specifies the number of the subinterface.
Step 2	(config-if)# **ipaddress***address mask*	Assigns the specified IP address and subnet mask to the interface or subinterface.
Step 3	Device(config-if)# **pvc** [*name*] *vpi* /*vci*	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for *vpi* /*vci* are: • *name*—(Optional) An arbitrary string that identifies this PVC. • *vpi*—Specifies the VPI ID. The valid range is 0 to 255. • *vci*—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is not supported.

	Command or Action	Purpose
		Note When using the **pvc** command, remember that the *vpi* /*vci* combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a *vpi* /*vci* combination that has been used on another subinterface, the Cisco IOS software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.
Step 4	Device(config-if-atm-vc)# **protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**] **Example:**	Configures the PVC for a particular protocol and maps it to a specific *protocol-address* . • *protocol*—Typically set to **ip**or **pppoe**, but other values are possible. **Note** PPP is not supported. • *protocol-address*—Destination address or virtual interface template for this PVC (if appropriate for the *protocol*). • **inarp** —Specifies that the PVC uses Inverse ARP to determine its address. • [**no**] **broadcast**—(Optional) Specifies that this mapping should (or should not) be used for broadcast packets.
Step 5	Device(config-if-atm-vc)# **inarp** *minutes*	(Optional) If using Inverse ARP, configures how often the PVC transmits Inverse ARP requests to confirm its address mapping. The valid range is 1 to 60 minutes, with a default of 15 minutes.
Step 6	Device(config-if-atm-vc)# **encapsulation** {**aal5mux**|**aal5nlpidaal5snap**}	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where: • **aal5mux** *protocol*—AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. Possible values for the *protocol* argument are as follows: • **aal5nlpid** —AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. • **aal5snap** —AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical

	Command or Action	Purpose
		link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default.
Step 7	Device(config-if-atm-vc)# **end**	Exits ATM VC configuration mode and returns to privileged EXEC mode.

Creating a PVC on a Point-to-Point Subinterface

Use point-to-point subinterfaces to provide each pair of routers with its own subnet. When you create a PVC on a point-to-point subinterface, the router assumes it is the only point-to-point PVC that is configured on the subinterface, and it forwards all IP packets with a destination IP address in the same subnet to this VC. To configure a point-to-point PVC, perform the following procedure beginning in global configuration mode:

SUMMARY STEPS

1. Device(config)# **interfaceatm***slot*/*subslot*/*port***.***subinterface***point-to-point**
2. Device(config-subif)# **ipaddress***address mask*
3. Device(config-subif)# **pvc** [*name*] *vpi* /*vci*
4. Device(config-if-atm-vc)# **protocol***protocol protocol-address* [[**no**] **broadcast**]
5. Device(config-if-atm-vc)# **encapsulation**{**aal5mux***protocol*|**aal5nlpid**|**aal5snap**}
6. Device(config-if)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **interfaceatm***slot*/*subslot*/*port***.***subinterface***point-to-point**	Creates the specified point-to-point subinterface on the given port on the specified ATM SPA, and enters subinterface configuration mode, where: • *slot*—Specifies the chassis slot number in the Cisco ASR 1000 Series Router where the SIP is installed. • *subslot*—Specifies the secondary slot of the SIP where the SPA is installed. • *port*—Specifies the number of the individual interface port on a SPA. • *subinterface*—Specifies the number of the subinterface.
Step 2	Device(config-subif)# **ipaddress***address mask*	Assigns the specified IP address and subnet mask to this subinterface.
Step 3	Device(config-subif)# **pvc** [*name*] *vpi* /*vci*	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for *vpi* /*vci* are: • *name*—(Optional) An arbitrary string that identifies this PVC.

	Command or Action	Purpose
		• *vpi*—Specifies the VPI ID. The valid range is 0 to 255. • *vci*—Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is unsupported on the Cisco ASR 1000 Series Routers. **Note** When using the **pvc** command, remember that the *vpi* /*vci* combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a *vpi* /*vci* combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.
Step 4	Device(config-if-atm-vc)# **protocol***protocol protocol-address* [[**no**] **broadcast**]	Configures the PVC for a particular protocol and maps it to a specific *protocol-address* . • *protocol*—Typically set to **ip** or **pppoe** for point-to-point subinterfaces, but other values are possible. **Note** PPP is not supported on the Cisco ASR 1000 Series Routers, and PPPoE is supported beginning in Cisco IOS XE Release 2.5. • *protocol-address*—Destination address or virtual template interface for this PVC (as appropriate for the specified *protocol*). • [**no**] **broadcast**—(Optional) Specifies that this mapping should (or should not) be used for broadcast packets. The **protocol** command also has an **inarp** option, but this option is not meaningful on point-to-point PVCs that use a manually configured address.
Step 5	Device(config-if-atm-vc)# **encapsulation**{**aal5mux***protocol*|**aal5nlpid**|**aal5snap**}	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where: • **aal5mux** *protocol*—AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. • **aal5nlpid** —(IP only) AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running

	Command or Action	Purpose
		ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. • **aal5snap** —AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default. **Note** Repeat Step 1 through Step 5 for each point-to-point subinterface to be configured on this ATM SPA.
Step 6	Device(config-if)# **end**	Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

Tip To verify the configuration and current status of all PVCs on a particular interface, you can also use the **showatmvcinterfaceatm** command.

Verifying a Multipoint PVC Configuration

To verify the configuration of a particular PVC, use the **show atm pvc** command:

```
Device# show atm pvc 1/120

ATM3/1/0.120: VCD: 1, VPI: 1, VCI: 120
UBR, PeakRate: 149760
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC status: Not Managed
ILMI VC status: Not Managed
InARP frequency: 15 minutes(s)
Transmit priority 3
InPkts: 1394964, OutPkts: 1395069, InBytes: 1833119, OutBytes: 1838799
InPRoc: 1, OutPRoc: 1, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 94964, OutAS: 95062
InPktDrops: 0,  OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Note To verify the configuration and current status of all PVCs on a particular interface, you can also use the **show atm vc interface** command.

Mapping a Protocol Address to a PVC

The ATM interface supports a static mapping scheme that identifies the network address of remote hosts or routers. This section describes how to map a PVC to an address, which is a required task for configuring a PVC.

Note If you enable or disable broadcasting directly on a PVC using the **protocol** command, this configuration will take precedence over any direct configuration using the **broadcast** command.

See examples of PVC configurations in the section "ATM Configuration Examples, on page 29".

To map a protocol address to a PVC, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)# protocol protocol protocol-address [[no] broadcast]`	Maps a protocol address to a PVC.

Configuring the AAL and Encapsulation Type

To configure the ATM adaptation layer (AAL) and encapsulation type, use the following command beginning in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)# encapsulation aal5 encap`	Configures the ATM adaptation layer (AAL) and encapsulation type. • For a list of AAL types and encapsulations supported for the *aal-encap* argument, refer to the **encapsulation aal5** command in the "ATM Commands" chapter of the *Cisco IOS Wide-Area Networking Command Reference*. The global default is AAL5 with SNAP encapsulation.

Configuring PVC Traffic Parameters

The supported traffic parameters are part of the following service categories: Constant Bit Rate (CBR), Unspecified Bit Rate (UBR), Variable Bit Rate Non Real-Time (VBR-NRT), and real-time Variable Bit Rate (VBR). Only one of these categories can be specified per PVC connection so if a new one is entered, it will replace the existing one.

Note The commands in this section are not supported on the ATM port adapter (PA-A1 series). The 1-port ATM-25 network module only supports UBR.

The *-pcr* and *-mcr* arguments are the peak cell rate and minimum cell rate, respectively. The *-scr* and *-mbs* arguments are the sustainable cell rate and maximum burst size, respectively.

To configure PVC traffic parameters, use one of the following commands beginning in interface-ATM-VC configuration mode:

Command	Purpose
`Router(config-if-atm-vc)# cbr peak_cell_rate_KBPS`	Configures the Constant Bit Rate (CBR).
`Router(config-if-atm-vc)# ubr output-pcr`	Configures the Unspecified Bit Rate (UBR).
`Router(config-if-atm-vc)# vbr-nrt output-pcr output-scr output-mbs`	Configures the Variable Bit Rate-Non Real Time (VBR-NRT) QOS.
`Router(config-if-atm-vc)# vbr-rt peak-rate average-rate burst`	Configures the real-time Variable Bit Rate (VBR). (Cisco MC3810 and Multiport T1/E1 ATM Network Module only.)

Enabling Inverse ARP

Inverse ARP is enabled by default when you create a PVC using the **pvc** command. Once configured, a protocol mapping between an ATM PVC and a network address is learned dynamically as a result of the exchange of ATM Inverse ARP packets.

Inverse ARP is supported on PVCs running IP or IPX and no static map is configured. If a static map is configured, Inverse ARP will be disabled.

When PVC discovery is enabled on an active PVC and the router terminates that PVC, the PVC will generate an ATM Inverse ARP request. This allows the PVC to resolve its own network addresses without configuring a static map.

Address mappings learned through Inverse ARP are aged out. However, mappings are refreshed periodically. This period is configurable using the **inarp** command, which has a default of 15 minutes.

You can also enable Inverse ARP using the **protocol** command. This is necessary only if you disabled Inverse ARP using the **no protocol** command. For more information about this command, refer to the "ATM Commands" chapter in the *Cisco IOS Wide-Area Networking Command Reference*.

For an example of configuring Inverse ARP, see the section "Enabling Inverse ARP Example, on page 31".

To enable Inverse ARP on an ATM PVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**[**.** *subinterface-number*{**multipoint** | **point-to-point**}]

2. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
3. Router(config-if-atm-vc)# **encapsulation aal5snap**
4. Router(config-if-atm-vc)# **inarp** *minutes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0[.** *subinterface-number*{**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)# interface atm number[. subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[1]
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Specifies an ATM PVC by name (optional) and VPI/VCI numbers.
Step 3	Router(config-if-atm-vc)# **encapsulation aal5snap**	Configures AAL5 LLC-SNAP encapsulation if it is not already configured.
Step 4	Router(config-if-atm-vc)# **inarp** *minutes*	(Optional) Adjusts the Inverse ARP time period.

Enabling ANCP on an ATM Interface

The **ancp enable** command should be configured only for the control VCs on which the Access Node Control Protocol (ANCP) message is sent from the DSLAM. Use the following procedure to enable ANCP on ATM interfaces. For an example of enabling ANCP, see the section Enabling ANCP on ATM Interfaces Example, on page 31.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ancp adjacency timer** *interval*
4. **interface atm** *slot* / *subslot* / *port* **.** *subinterface*
5. **ip address** *ip-address mask*
6. **pvc** *vpi* / *vci*

7. **ancp enable**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ancp adjacency timer** *interval* **Example:** `Router(config)# ancp adjacency timer 100`	Sets the ANCP adjacency timer interval, which specifies the amount of time to wait before sending an ANCP hello packet to the DSLAM. • Valid values are defined in units of 100 milliseconds (ms). Default: 100 (10 seconds).
Step 4	**interface atm** *slot* / *subslot* / *port* **.** *subinterface* **Example:** `Router(config)# interface atm 2/0/1.1`	Creates or modifies a subinterface and enters subinterface configuration mode.
Step 5	**ip address** *ip-address mask* **Example:** `Router(config-subif)# ip address 10.16.1.2 255.255.0.0`	Assigns an IP address and subnet mask to the subinterface.
Step 6	**pvc** *vpi* / *vci* **Example:** `Router(config-subif)# pvc 2/100`	Enables an ANCP connection over ATM PVC and enters ATM virtual circuit configuration mode.
Step 7	**ancp enable** **Example:** `Router(config-if-atm-vc)# ancp enable`	Enables ANCP on the interface where IP is configured.
Step 8	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode.

Configuring Loopback Cells to Verify Connectivity

You can optionally configure the PVC to generate end-to-end F5 OAM loopback cells to verify connectivity on the virtual circuit. The remote end must respond by echoing back such cells. If OAM response cells are missed (indicating the lack of connectivity), the PVC state goes down. If all the PVCs on a subinterface go down, the subinterface goes down.

For information about managing PVCs using OAM, see the section "Configuring OAM Management for PVCs, on page 26".

For an example of OAM loopback cell generation, see the section "Configuring Loopback Cells Example, on page 32".

To configure transmission of end-to-end F5 OAM cells on a PVC, use the following commands in interface-ATM-VC configuration mode:

SUMMARY STEPS

1. Router(config-if-atm-vc)# **oam-pvc** [**manage**] *frequency*
2. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if-atm-vc)# **oam-pvc** [**manage**] *frequency*	Configures transmission of end-to-end F5 OAM loopback cells on a PVC, specifies how often loopback cells should be sent, and optionally enables OAM management of the connection.
Step 2	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for verifying connectivity of a PVC connection. This command is only supported if OAM management is enabled. • Use the *up-count*argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. Use the *down-count*argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down a PVC. Use the *retry-frequency* argument to specify the frequency (in seconds) that end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-pvc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the PVC is down.

Configuring Broadcast on a PVC

To send duplicate broadcast packets for all protocols configured on a PVC, use the following command in interface-ATM-VC configuration mode:

Note If you enable or disable broadcasting directly on a PVC using the **protocol** command, this configuration will take precedence over any direct configuration using the **broadcast** command.

Command	Purpose
`Router(config-if-atm-vc)# broadcast`	Sends duplicate broadcast packets for all protocols configured on a PVC.

Configuring a PVC on a Multipoint Subinterface

Creating a multipoint subinterface allows you to create a point-to-multipoint PVC that can be used as a broadcast PVC for all multicast requests. To create a PVC on a multipoint subinterface, use the following procedure beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot/subslot/port.subinterface* **multipoint**
2. Router(config-subif)# **ip address** *address mask*
3. Router(config-subif)# **no ip directed-broadcast**
4. Router(config-subif)# **pvc** [*name*] *vpi /vci*
5. Router(config-if-atm-vc)# **protocol** *protocol* {*protocol-address* | **inarp**} **broadcast**
6. Router(config-if-atm-vc)# **inarp** *minutes*
7. Router(config-if-atm-vc)# **encapsulation**{**aal5mux***protocol*|**aal5nlpidaal5snap**}
8. Router(config-if-atm-vc)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot/subslot/port.subinterface* **multipoint**	Creates the specified point-to-multipoint subinterface on the given port on the specified ATM SPA, and enters subinterface configuration mode, where: • *slot* —Specifies the chassis slot number where the SIP is installed. • *subslot* —Specifies the secondary slot of the SIP where the SPA is installed. • *port* —Specifies the number of the individual interface port on a SPA. • *subinterface* —Specifies the number of the subinterface.

	Command or Action	Purpose
Step 2	Router(config-subif)# **ip address** *address mask*	Assigns the specified IP address and subnet mask to this subinterface.
Step 3	Router(config-subif)# **no ip directed-broadcast**	(Optional) Disables the forwarding of IP directed broadcasts, which are sometimes used in denial of service (DOS) attacks.
Step 4	Router(config-subif)# **pvc** [*name*] *vpi* /*vci*	Configures a new ATM PVC by assigning its VPI/VCI numbers and enters ATM VC configuration mode. The valid values for *vpi* /*vci* are: • *name* —(Optional) An arbitrary string that identifies this PVC. • *vpi* —Specifies the VPI ID. The valid range is 0 to 255. • *vci* —Specifies the VCI ID. The valid range is 32 to 65535. Values 1 to 31 are reserved and should not be used, except for 5 for the QSAAL PVC and 16 for the ILMI PVC. ILMI is not supported. **Note** When using the **pvc** command, remember that the *vpi* /*vci* combination forms a unique identifier for the interface and all of its subinterfaces. If you specify a *vpi* /*vci* combination that has been used on another subinterface, the Cisco IOS XE software assumes that you want to modify that PVC's configuration and automatically switches to its parent subinterface.
Step 5	Router(config-if-atm-vc)# **protocol** *protocol* {*protocol-address* | **inarp**} **broadcast**	Configures the PVC for a particular protocol and maps it to a specific *protocol-address* . • *protocol* —Typically set to **ip**or **pppoe**, but other values are possible. **Note** PPP is not supported • *protocol-address* —Destination address or virtual template interface for this PVC (if appropriate for the *protocol*). • **inarp** —Specifies that the PVC uses Inverse ARP to determine its address. • **broadcast** — Specifies that this mapping should be used for multicast packets.
Step 6	Router(config-if-atm-vc)# **inarp** *minutes*	(Optional) If using Inverse ARP, configures how often the PVC transmits Inverse ARP requests to confirm its address

	Command or Action	Purpose
		mapping. The valid range is 1 to 60 minutes, with a default of 15 minutes.
Step 7	Router(config-if-atm-vc)# **encapsulation** {**aal5mux***protocol*|**aal5nlpidaal5snap**}	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type, where: • **aal5mux** *protocol* —AAL and encapsulation type for multiplex (MUX)-type VCs. A protocol must be specified when you use this encapsulation type. • **aal5nlpid** —(IP only) AAL and encapsulation type that allows ATM interfaces to interoperate with High-Speed Serial Interfaces (HSSIs) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). Supported on ATM PVCs only. • **aal5snap** —AAL and encapsulation type that supports Inverse Address Resolution Protocol (ARP). Logical link control/Subnetwork Access Protocol (LLC/SNAP) precedes the protocol datagram. This is the default. **Note** Repeat Step 1 through Step 7 for each multipoint subinterface to be configured on this ATM SPA.
Step 8	Router(config-if-atm-vc)# **end**	Exits interface configuration mode and returns to privileged EXEC mode.

Assigning a VC Class to a PVC

By creating a VC class, you can preconfigure a set of default parameters that you may apply to a PVC. To create a VC class, refer to the section "Configuring VC Classes, on page 23".

Once you have created a VC class, use the following command in interface-ATM-VC configuration mode to apply the VC class to a PVC:

Command	Purpose
`Router(config-if-atm-vc)#` **`class-vc`** *`vc-class-name`*	Applies a VC class to a PVC. • The *vc-class-name* argument is the same as the *name* argument you specified when you created a VC class using the **vc-class atm** command. Refer to the section "Configuring VC Classes, on page 23" for a description of how to create a VC class.

Configuring PVC Trap Support

You can configure the PVC to provide failure notification by sending a trap when a PVC on an ATM interface fails or leaves the UP operational state.

PVC Failure Notification

Only one trap is generated per hardware interface, within the specified interval defined by the interval "atmIntPvcNotificationInterval". If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the interval has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No trap is generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

PVC Status Tables

When PVC trap support is enabled, the SNMP manager can poll the SNMP agent to get PCV status information. The table "atmInterfaceExtTable" provides PVC status on an ATM interface. The table "atmCurrentlyFailingPVclTable" provides currently failing and previously failed PVC time-stamp information.

Note PVC traps are only supported on permanent virtual circuit links (PVCLs), not permanent virtual path links (PVPLs).

Prerequisites

Before you enable PVC trap support, you must configure SNMP support and an IP routing protocol on your router. See the "ATM Configuration Examples, on page 29" section.

For more information about configuring SNMP support, refer to the chapter "Configuring SNMP Support" in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about configuring IP routing protocols, refer to the *Cisco IOS IP Routing Protocols Configuration Guide*.

To receive PVC failure notification and access to PVC status tables on your router, you must have the Cisco PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB.my compiled in your NMS application. You can find this MIB on the Web at Cisco's MIB websiteat the URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Enabling PVC Trap Support

When you configure PVC trap support, you must also enable OAM management on the PVC.

For more information on OAM management, see the section "Configuring OAM Management for PVCs, on page 26" later in this chapter.

The new objects in this feature are defined in the IETF draft The Definitions of Managed Objects for ATM Management , which is an extension to the AToM MIB (RFC 1695).

For an example of configuring PVC trap support, see the section "Configuring PVC Trap Support Example, on page 32".

To enable PVC trap support and OAM management, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **snmp-server enable traps atm pvc interval** *seconds***fail-interval** *seconds*
2. Do one of the following:

- Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}]
-
-
- Router(config)# **interface atm** *slot* / *port-adapter* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}]

3. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
4. Router(config-if-atm-vc)# **oam-pvc manage**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **snmp-server enable traps atm pvc interval** *seconds***fail-interval** *seconds*	Enables PVC trap support.
Step 2	Do one of the following: • Router(config)# **interface atm** *slot* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* / *port-adapter* **/0[.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm number[. subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate form of the **interface atm** command.[2]
Step 3	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Enables the PVC.
Step 4	Router(config-if-atm-vc)# **oam-pvc manage**	Enables end-to-end OAM management for an ATM PVC.

Configuring VC Classes

A VC class is a set of preconfigured VC parameters that you configure and apply to a particular VC or ATM interface. You may apply a VC class to an ATM main interface, subinterface, or PVC. For example, you can create a VC class that contains VC parameter configurations that you will apply to a particular PVC. You might create another VC class that contains VC parameter configurations that you will apply to all VCs configured on a particular ATM main interface or subinterface. Refer to the "ATM Configuration Examples, on page 29" section for examples of VC class configurations.

Creating a VC Class

To create a VC class, use the following command in global configuration mode:

For examples of creating VC classes, see the section "Creating a VC Class Example, on page 32".

Command	Purpose
`Router(config)# vc-class atm name`	Creates a VC class and enters vc-class configuration mode.

Configuring VC Parameters

After you create a VC class and enter vc-class configuration mode, configure VC parameters using one or more of the following commands:

- **broadcast**
- **cbr**
- **encapsulation aal5**
- **idle-timeout**
- **inarp**
- **oam-pvc**
- **oam retry**
- **protocol**
- **ubr**
- **vbr-nrt**

Refer to the sections "Configuring PVCs, on page 8" and "Configuring PVC Trap Support, on page 21" for descriptions of how to configure these commands for PVCs.

For examples of creating VC classes, see the section "Creating a VC Class Example, on page 32".

Applying a VC Class on an ATM PVC

Once you have created and configured a VC class, you can apply it directly on an ATM PVC, or you can apply it on an ATM interface or subinterface.

To apply a VC class directly on an ATM PVC use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **pvc** [*name*] *vpi* / *vci*
2. Router(config-if-atm-vc)# **class-vc***vc-class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Specifies an ATM PVC
Step 2	Router(config-if-atm-vc)# **class-vc***vc-class-name*	Applies a VC class directly on the PVC.

Applying a VC Class on an ATM Interface

To apply a VC class on an ATM main interface or subinterface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **class-int** *vc-class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] • • • Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)# interface atm number[. subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[3]
Step 2	Router(config-if)# **class-int** *vc-class-name*	Applies a VC class on an the ATM main interface or subinterface.

Configuring VC Management

When you configure VC management, you enable the router to detect VC connections and disconnections automatically. This notifies protocols to reroute packets immediately, preventing protocols from waiting for unpredictable and relatively long timeout periods.

You may use operation, administration, and maintenance (OAM) to manage your PVCs, and decide which method is reliable in your particular network.

When a PVC goes down, route caches for protocols configured on that PVC are cleared (or flushed) so that new routes may be learned. The route cache flush is applied on the PVC's interface. When all PVCs on a subinterface go down, VC management shuts down the subinterface in addition to flushing route caches. ATM hardware must keep the PVC active, however, so that OAM cells may flow. When any PVC on a subinterface comes up, the subinterface is brought up.

VC management using OAM is referred to as OAM management.

Configuring OAM Management for PVCs

OAM management may be enabled for PVCs.

By default, end-to-end F5 OAM loopback cell generation is turned off for each PVC. A PVC is determined as down when any of the following is true on that PVC:

- The router does not receive a loopback reply after a configured number of retries of sending end-to-end F5 OAM loopback cells.
- The router receives a Virtual Circuit-Alarm Indication Signals (VC-AIS) cell.
- The router receives a Virtual Circuit-Remote Detect Indicator (VC-RDI) cell.

A PVC is determined as up when all of the following are true on that PVC:

- The router receives a configured number of successive end-to-end F5 OAM loopback cell replies.
- The router does not receive VC-AIS cell for 3 seconds.
- The router does not receive VC-RDI cell for 3 seconds.

To configure OAM management for an ATM PVC, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
   -
   -
   - Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}]
2. Router(config-if)# **pvc** [*name*] *vpi* **/** *vci*
3. Router(config-if-atm-vc)# **oam-pvc manage** [*frequency*]
4. Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0**[**.** *subinterface-number* {**multipoint**	**point-to-point**}] •	Specifies the ATM interface using the appropriate format of the **interface atm** command.[4]

	Command or Action	Purpose
	• • Router(config)# **interface atm** *slot* / *port-adapter* /**0**[**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** **Example:** **Example:** `Router(config)# Router(config)# interface atm number[. subinterface-number {multipoint | point-to-point}]`	
Step 2	Router(config-if)# **pvc** [*name*] *vpi* / *vci*	Specifies the ATM PVC.
Step 3	Router(config-if-atm-vc)# **oam-pvc manage** [*frequency*]	Enables OAM management on the PVC.
Step 4	Router(config-if-atm-vc)# **oam retry** *up-count down-count retry-frequency*	(Optional) Specifies OAM management parameters for re-establishing and removing a PVC connection. • Use the *up-count*argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a PVC connection state to up. Use the *down-count*argument to specify the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to tear down a PVC. Use the *retry-frequency* argument to specify the frequency (in seconds) that end-to-end F5 OAM loopback cells should be transmitted when a change in UP/DOWN state is being verified. For example, if a PVC is up and a loopback cell response is not received after the *frequency* (in seconds) specified using the **oam-pvc** command, then loopback cells are sent at the *retry-frequency* to verify whether or not the PVC is down.

Configuring Classical IP and Inverse ARP in a PVC Environment

The ATM Inverse ARP mechanism is applicable to networks that use PVCs, where connections are established but the network addresses of the remote ends are not known. A server function is *not* used in this mode of operation.

By default, Inverse ARP datagrams will be sent on this virtual circuit every 15 minutes. To adjust the Inverse ARP time period, use the **inarp** *minutes* command in interface-ATM-VC configuration mode.

Note The ATM ARP mechanism works with IP only. The Inverse ATM ARP mechanism works with IP and IPX only. For all other protocols, the destination address must be specified.

In a PVC environment, the ATM Inverse ARP mechanism is enabled by default for IP and IPX when you use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Do one of the following:
   - Router(config)# **interface atm** *slot* **/0**
   -
   -
   - Router(config)# **interface atm** *slot* **/** *port-adapter* **/0**
2. Router(config-if)# **ip address** *address mask*
3. Router(config-if)# **pvc** [*name*] *vpi* **/** *vci*
4. Router(config-if-atm-vc)# **no shutdown**
5.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Router(config)# **interface atm** *slot* **/0** • • • Router(config)# **interface atm** *slot* **/** *port-adapter* **/0** **Example:** **Example:** **Example:** `Router(config)# interface atm number`	Specifies the ATM interface using the appropriate format of the **interface atm** command.[5]
Step 2	Router(config-if)# **ip address** *address mask*	Specifies the IP address of the interface.
Step 3	Router(config-if)# **pvc** [*name*] *vpi* **/** *vci*	Creates a PVC.
Step 4	Router(config-if-atm-vc)# **no shutdown**	Enables the ATM interface.
Step 5		Repeat Step 3 for each PVC you want to create.

Customizing the ATM Interface

You can customize the ATM interface. The features you can customize have default values that will most likely suit your environment and probably need not be changed. However, you might need to enter configuration commands, depending upon the requirements for your system configuration and the protocols you plan to route on the interface.

Configuring MTU Size

Each interface has a default maximum packet size or maximum transmission unit (MTU) size. For ATM interfaces, this number defaults to 4470 bytes. The MTU can be set on a per-sub-interface basis as long as the interface MTU is as large or larger than the largest subinterface MTU.

To set the maximum MTU size, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# mtu bytes`	Sets the maximum MTU size.

ATM Configuration Examples

The examples in the following sections illustrate how to configure ATM for the features described in this chapter. The examples below are presented in the same order as the corresponding configuration task sections:

Creating a PVC Example

The following example shows how to create a PVC on an ATM main interface with AAL5/MUX encapsulation configured and a VBR-NRT QOS specified. For further information, refer to sections “Creating a PVC” and “Configuring PVC Traffic Parameters”.

```
interface 2/0
 pvc cisco 1/40
 encapsulation aal5mux ip
 vbr-nrt 100000 50000 20
 exit
```

PVC with AAL5 and LLC SNAP Encapsulation Examples

The following example shows how to create a PVC 0/50 on ATM interface 3/0. It uses the global default LLC/SNAP encapsulation over AAL5. The interface is at IP address 1.1.1.1 with 1.1.1.5 at the other end of the connection. For further information, refer to the sections “Creating a PVC” and “Mapping a Protocol Address to a PVC".

```
interface atm 3/0
 ip address 1.1.1.1 255.255.255.0
 pvc 0/50
 protocol ip 1.1.1.5 broadcast
 exit
!
 ip route-cache cbus
```

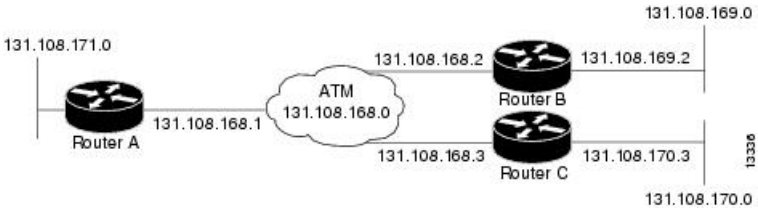
The following example is a typical ATM configuration for a PVC:

```
interface atm 4/0
 ip address 172.21.168.112 255.255.255.0
 atm maxvc 512
 pvc 1/51
 protocol ip 171.21.168.110
 exit
!
 pvc 2/52
 protocol decnet 10.1 broadcast
 exit
!
 pvc 3/53
 protocol clns 47.004.001.0000.0c00.6e26.00 broadcast
 exit
!
 decnet cost 1
 clns router iso-igrp comet
 exit
!
router iso-igrp comet
 net 47.0004.0001.0000.0c00.6666.00
 exit
!
router igrp 109
 network 172.21.0.0
 exit
!
ip domain-name CISCO.COM
```

PVCs in a Fully Meshed Network Example

The figure below illustrates a fully meshed network. The configurations for routers A, B, and C follow the figure. In this example, the routers are configured to use PVCs. Fully meshed indicates that any workstation can communicate with any other workstation. Note that the two **protocol** statements configured in router A identify the ATM addresses of routers B and C. The two **protocol**statements in router B identify the ATM addresses of routers A and C. The two **protocol** statements in router C identify the ATM addresses of routers A and B. For further information, refer to the sections “Creating a PVC” and “Mapping a Protocol Address to a PVC”.

Figure 3: Fully Meshed ATM Configuration Example



Router A

```
ip routing
!
interface atm 4/0
 ip address 131.108.168.1 255.255.255.0
 pvc 0/32
```

```
 protocol ip 131.108.168.2 broadcast
 exit
!
 pvc 0/33
 protocol ip 131.108.168.3 broadcast
 exit
```

Router B

```
ip routing
!
interface atm 2/0
 ip address 131.108.168.2 255.255.255.0
 pvc 0/32
 protocol ip 131.108.168.1 broadcast
 exit
!
 pvc 0/34
 protocol ip 131.108.168.3 broadcast
 exit
```

Router C

```
ip routing
!
interface atm 4/0
 ip address 131.108.168.3 255.255.255.0
 pvc 0/33
 protocol ip 131.108.168.1 broadcast
 exit
!
 pvc 0/34
 protocol ip 131.108.168.2 broadcast
 exit
```

Enabling Inverse ARP Example

The following example shows how to enable Inverse ARP on an ATM interface and specifies an Inverse ARP time period of 10 minutes.

```
interface atm 2/0/0.1
 pvc 1/32
 inarp 10
 exit
```

Enabling ANCP on ATM Interfaces Example

The following example shows how to enable ANCP on an ATM subinterface. In the example, ANCP is enabled on ATM subinterface 2/0/1.1.

```
interface ATM2/0/0.1 point-to-point
      description ANCP Link to one DSLAM
      no ip mroute-cache
      ip address 192.168.0.2 255.255.255.252
      pvc 254/32
        protocol ip 192.168.0.1
```

```
ancp enable
no snmp trap link-status
```

Configuring Loopback Cells Example

The following example shows how to enable OAM management on an ATM PVC. The PVC is assigned the name routerA and the VPI and VCI are 0 and 32, respectively. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions. For further information, refer to the section "Enabling ANCP on an ATM Interface, on page 16".

```
interface atm 2/0
 pvc routerA 0/32
 oam-pvc manage 3
 oam retry 5 5 10
```

Configuring PVC Trap Support Example

The following example shows how to configure PVC trap support on your Cisco router:

```
!For PVC trap support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 171.69.61.90 public

Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.21.0.0
!
!Enable PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
!
! Now if PVC 0/1 goes down, host 171.69.61.90 will receive traps.
```

For further information, refer to the "Configuring PVC Trap Support, on page 21" section.

Creating a VC Class Example

The following example shows how to create a VC class named main and how to configure UBR and encapsulation parameters. For further information, refer to the sections "Creating a VC Class, on page 23" and "Configuring VC Parameters, on page 24".

```
vc-class atm main
 ubr 10000
 encapsulation aal5mux ip
```

The following example shows how to create a VC class named sub and how to configure UBR and PVC management parameters. For further information, refer to the sections "Creating a VC Class, on page 23" and "Configuring VC Parameters, on page 24".

```
vc-class atm sub
 ubr 15000
 oam-pvc manage 3
```

The following example shows how to create a VC class named pvc and how to configure VBR-NRT and encapsulation parameters. For further information, refer to the sections "Creating a VC Class, on page 23" and "Configuring VC Parameters, on page 24"".

```
vc-class atm pvc
 vbr-nrt 10000 5000 64
 encapsulation aal5snap
```

Applying a VC Class Example

The following example shows how to apply the VC class named main to the ATM main interface 4/0. For further information, refer to the section "Applying a VC Class on an ATM PVC, on page 24".

```
interface atm 4/0
 class-int main
 exit
```

The following example shows how to apply the VC class named sub to the ATM subinterface 4/0.5:

```
interface atm 4/0.5 multipoint
 class-int sub
 exit
```

The following example shows how to apply the VC class named pvc directly on the PVC 0/56:

```
interface atm 4/0.5 multipoint
 pvc 0/56
 class-vc pvc
 exit
```

OAM Management on an ATM PVC Example

The following example shows how to enable OAM management on an ATM PVC. The PVC is assigned the name routerA and the VPI and VCI are 0 and 32, respectively. OAM management is enabled with a frequency of 3 seconds between OAM cell transmissions. For further information, refer to the section "Configuring OAM Management for PVCs, on page 26".

```
interface atm 2/0
 pvc routerA 0/32
 oam-pvc manage 3
 oam retry 5 5 10
!
interface atm 4/0.1 point-to-point
 pvc 0/35
 exit
```

No **map-group** and **map-list** commands are needed for IP.

```
interface atm 4/0
 ip address 1.1.1.1 255.0.0.0
 pvc 1/33
 pvc 1/34
 pvc 1/35
 bridge-group 1
!
bridge 1 protocol dec
```

Example Configuring a PVC Bundle

```
Device1:
interface ATM0/0/0.1 point-to-point
ip address 10.0.0.1 255.255.255.0
bundle test
  encapsulation aal5snap
  oam-bundle manage
  pvc-bundle 0/32
   vbr-rt 19000 15000 5000
   precedence 7
  pvc-bundle 1/33
   ubr 2480
   precedence 6
  pvc-bundle 1/34
   ubr 4890
   precedence 3-5
  pvc-bundle 1/35
!
Device2:

interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.255.255.0
bundle test
  encapsulation aal5snap
  oam-bundle manage
  pvc-bundle 0/32
   vbr-rt 19000 15000 5000
   precedence 7
  pvc-bundle 1/33
   ubr 2480
   precedence 6
  pvc-bundle 1/34
   ubr 4890
   precedence 3-5
  pvc-bundle 1/35
!
```

PVC on a Point-to-Point Subinterface Configuration Example

```
interface ATM5/0/0.9 point-to-point
 mtu 4474
 bandwidth 34000
 ip vrf forwarding vrfexample
 ip address 192.0.2.1 255.255.255.0
 ip mtu 4470
 pvc 11/105
  ubr 38
  oam-pvc manage
  encapsulation aal5snap
 !
interface ATM5/0/0.11 point-to-point
 mtu 4474
 bandwidth 7000
 ip address 192.0.2.2 255.255.255.0
 ip mtu 4470
 pvc 100/50
  cbr 7000
  encapsulation aal5snap
```

```
service-policy input Leased_Line_Ingress
max-reserved-bandwidth 100
```

Monitoring and Maintaining the ATM Interface

After configuring an ATM interface, you can display its status. You can also display the current state of the ATM network and connected virtual circuits. To show current virtual circuits and traffic information, use the following commands in EXEC mode:

Command	Purpose
`Router# show arp`	Displays entries in the ARP table.
`Router# show atm class-links {vpi / vci | name}`	Displays PVC parameter configurations and where the parameter values are inherited from.

`Router# show atm interface atm slot /0`
 	
`Router# show atm interface atm slot / port-adapter /0`
 	
`Router# show atm interface atm number`
	Displays ATM-specific information about the ATM interface using the appropriate format of the **show atm interface atm** command.[6]

`Router# show atm map`	Displays the list of all configured ATM static maps to remote hosts on an ATM network.
`Router# show atm pvc [vpi / vci | name | interface atm interface_number]`	Displays all active ATM PVCs and traffic information.
`Router# show atm traffic`	Displays global traffic information to and from all ATM networks connected to the router, OAM statistics, and a list of counters of all ATM traffic on this router.
`Router# show atm vc [vcd-number | [range lower-limit-vcd upper-limit-vcd] [interface ATM interface-number] [detail [prefix {vpi/vci | vcd | interface | vc_name}]] [connection-name] | signalling [freed-svcs | [cast-type {p2mp | p2p}] [detail] [interface ATM interface-number]] | summary ATM interface-number]`	Displays all active ATM virtual circuits (PVCs) and traffic information. **Note** The SVCs and the **signalling** keyword are not supported.
`Router# show interfaces atm controller.port-channels.subinterface`	Displays statistics for the ATM interface using the appropriate format of the **show interfaces atm** command.

Command	Purpose
`Router# show network-clocks`	Displays the clock signal sources and priorities that you established on the router.

[6] To determine the correct form of the interface atm command, consult your ATM network module, port adapter, or router documentation.

Feature Information for Configuring ATM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for Configuring ATM

Feature Name	Releases	Feature Information
Configuring ATM, ATM Sub-interface Multipoint	Cisco IOS Release 2.5.0	

Feature Name	Releases	Feature Information
		ATM supports two types of interfaces: point-to-point and multipoint. • Point-to-point subinterface--With point-to-point subinterfaces, each pair of devices has its own subnet. If you put the PVC on a point-to-point subinterface, the device assumes that there is only one point-to-point PVC configured on the subinterface. Therefore, any IP packets with a destination IP address in the same subnet are forwarded on this virtual circuit (VC). This is the simplest way to configure the mapping and is therefore the recommended method. • Multipoint networks--Multipoint networks have three or more devices in the same subnet. If you put the PVC in a point-to-multipoint subinterface or in the main interface (which is multipoint by default), you need to either configure a static mapping or enable inverse Address Resolution Protocol (ARP) for dynamic mapping. ANCP needs to be enabled on ATM interface when message is sent from the DSLAM. The following commands were introduced or modified: **pvc**, **protocol**, **cbr**, **ubr**, **encapsulation aal5snap**, **interface atm**, **ip address**, **inarp**, **oam-pvc manage**, **oam-retry**, **class-vc**, **snmp-server enable traps**, **vc-class atm**, **class-int**, **mtu**, **show atm class-links**, **show atm interface**

Feature Name	Releases	Feature Information
		atm, **show atm map**, **show atm pvc**, **show atm traffic**, **show atm vc**, **show network-clocks**, ancp enable, ancp neighbor.
IP Multicast over ATM PVC Bundle	Cisco IOS Release XE 3.7S	ATM VC bundle management allows you to configure multiple VCs that have different QoS characteristics between any pair of ATM-connected devices. No new commands were introduced or modified.

Additional References

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*
ATM SPAs	"Overview of ATM SPAs" in the *Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide*
Configuring IP to ATM class of service (CoS)	• "IP to ATM CoS Overview" • "Configuring IP to ATM CoS"
Configuring PPP over Ethernet (PPPoE) over ATM	"Configuring PPPoE over ATM"

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

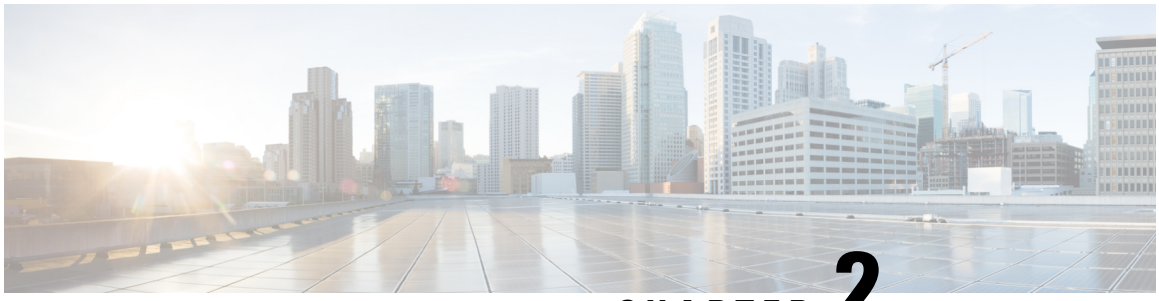
MIB	MIBs Link
• Cisco PVC trap MIB - CISCO-IETF-ATM2-PVCTRAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport



CHAPTER 2

ATM Conditional Debug Support

Most ATM debugging commands are implemented either at the system level or at the interface level. The ATM Conditional Debug Support feature allows debugging to be limited specifically to an ATM interface, to a virtual channel identifier (VCI), or to a virtual path identifier/virtual channel identifier (VPI/VCI) pair, through use of the **debug condition interface** command.

Prerequisites for ATM Conditional Debug Support

One or more ATM-encapsulated interfaces must be enabled, and one or more of the following **debug** commands must be enabled, to use the ATM Conditional Debug Support feature:

- **debug atm arp**
- **debug atm counters**
- **debug atm errors**
- **debug atm events**
- **debug atm oam**
- **debug atm packet**
- **debug atm state**

Restrictions for ATM Conditional Debug Support

- Only the ATM debugging commands listed in thePrerequisites for ATM Conditional Debug Support, on page 41 section can use the ATM Conditional Debug Support feature.

- Conditional debugging for virtual circuits (VCs) can be enabled only for permanent virtual circuits (PVCs). Switched virtual circuits (SVCs) are not supported.

Information About ATM Conditional Debug Support

ATM Debugging Extended to the VC Level

The ATM **debug** commands are implemented either at the interface level or at the system level. The **debug** command output at these levels is not very useful when the user is interested in a particular set of virtual circuits (VCs).

The Cisco IOS XE software has the infrastructure to support conditional debugging based on various filters that are set at the command-line interface (CLI). The conditional debugging infrastructure can filter out or suppress unwanted messages from the output of any existing **debug** command. The ATM Conditional Debug Support feature extends this infrastructure to support conditional debugging at the ATM VC level by extending the **debug condition interface** command with keywords that address specific virtual circuits. This feature can be implemented on top of conventional debugging, so that backward compatibility is ensured and at the same time applications can take advantage of conditional debugging where required. However, the extended **debug condition interface** command has priority over the older version of the command; that is, a debug condition setting using the older **debug condition interface** command will be discarded as soon as a new debug condition is enabled on a virtual circuit.

How to Configure ATM Conditional Debugging on ATM Interfaces

Enabling Debugging for the ATM Interface

Perform this task to enable conditional debugging on a set of specified interfaces.

Before you begin

You must enable ATM debugging and specify the conditions (interface, VCI, or VPI/VCI pair) for the ATM Conditional Debug Support feature to work.

SUMMARY STEPS

1. **enable**
2. **debug atm** [**arp** | **counters** | **errors** | **events** | **oam** | **packet** | **state**]
3. **debug condition interface** *interface-type interface-number* [**vc** {*vci* | *vpi* / *vci*}]

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**debug atm** [**arp** | **counters** | **errors** | **events** | **oam** | **packet** | **state**] **Example:** `Router# debug atm state`	Displays various ATM events.
Step 3	**debug condition interface** *interface-type interface-number* [**vc** {*vci* | *vpi* / *vci*}] **Example:** `Router# debug condition interface ATM1/1/0 vc 10/100`	Limits output for debugging according to the interface or ATM VC number.

Configuration Examples for ATM Conditional Debug Support

Enabling Debugging for an ATM Interface and VPI VCI Pair Example

The following example shows how to enable an ATM interface, specify an IP address for the interface, enable conditional debugging for that interface with a VPI/VCI pair of 10/100, and verify that debugging has been enabled:

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm 1/1/0.100 point-to-point

Router(config-if)# ip address 10.0.0.5 255.255.255.0
Router(config-if)# pvc 10/100

Router(config-if-atm-vc)# no shutdown

Router(config-if)# exit

Router(config)# exit

Router#
Router# debug atm state

ATM VC States debugging is on
Router# debug condition interface ATM1/1/0 vc 10/100

Condition 1 set
Router#
```

Enabling Debugging for a Specific VCI Example

The following example shows how to enable conditional debugging on a specific VCI. Note that when you enable conditional debugging on a specific VCI alone, the VPI value is automatically set to 0.

```
Router# debug condition interface atm 1/0 vc 4335
Condition 1 set
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm 1/0
Router(config-if)# pvc 4335
Router(config-if-atm-vc)# end
Router#
*Jul 12 21:46:52.487: atmdx_setup_vc(ATM1/0): vc=5, vpi=0, vci=4335,  config_status=0
*Jul 12 21:46:52.487: atmdx_setup_cos(ATM1/0): vc=5, wred_name=, max_q=0
*Jul 12 21:46:52.487: ATM VC Debug: Condition 1, atm-vc 0/4335 AT1/0 triggered, count 1
*Jul 12 21:46:52.487: ATM1/0 Current Active VC count 4

*Jul 12 21:46:52.487:  ATM VC notification event 0
*Jul 12 21:46:52.487: atmdx_platform_set_vc_state(ATM1/0): Setting the VC 5 state to UP
*Jul 12 21:46:52.487: ATM: PVC activated, ATM1/0 VCD 5 (0/4335)
*Jul 12 21:46:52.487:  ATM VC notification event 2
*Jul 12 21:46:52.487: %SYS-5-CONFIG_I: Configured from console by console
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE

           VCD /                                                Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC      Kbps   Kbps Cells St
1/0        1               0    16 PVC     ILMI       UBR  149760              UP
1/0.10     4               0   100 PVC     SNAP       UBR  149760              UP
1/0        5               0  4335 PVC     SNAP       UBR  149760              UP
1/0.1      one             1    40 PVC     SNAP       UBR  149760              UP
1/0        2               3   100 PVC-A   SNAP       VBR    1000   1000     0 IN
4/ima1     1              23    34 PVC     SNAP       UBR       0              IN
```

Additional References

Related Documents

Related Topic	Document Title
Conditionally triggered debugging	"Conditionally Triggered Debugging" chapter in the *Cisco IOS Debug Command Reference*
ATM Overview	Overview of the ATM SPAs
ATM commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples.	*Cisco IOS Asynchronous Transfer Mode Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

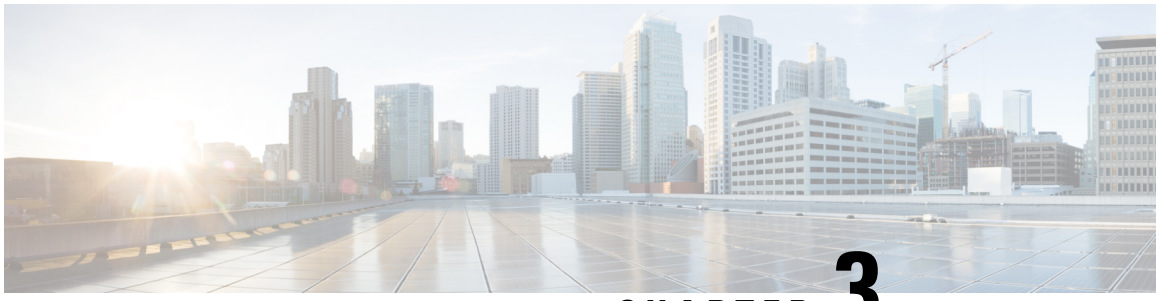
Feature Information for ATM Conditional Debug Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2: Feature Information for ATM Conditional Debug Support

Feature Name	Releases	Feature Information
ATM Conditional Debug Support	Cisco IOS XE Release 2.3	ATM Conditional Debug Support feature allows debugging to be limited specifically to an ATM interface, to a VCI, or to a VPI/VCI pair. The following commands are introduced or modified in the feature: **debug condition interface**, **show debug**.



CHAPTER 3

ATM Multilink PPP Support on Multiple VCs

The ATM Multilink PPP Support on Multiple VCs feature facilitates traffic load balancing on high-speed virtual circuits (VCs) using multilink PPP (MLP) over Frame Relay and ATM. It also facilitates traffic load balancing by using MLP to combine packet datagrams on high-speed VCs as a means of transporting both the voice and data traffic more efficiently.

Restrictions for ATM Multilink PPP Support

The ATM Multilink PPP Support on Multiple VCs feature does not support the following commands and functionality. The configuration accepts these commands, but the commands have no effect:

- **ppp interleave**
- **ppp multilink fragment-delay**

The ATM Multilink PPP Support on Multiple VCs feature does not support the link fragmentation and interleaving (LFI) functionality.

Information About ATM Multilink PPP Support

ATM Multilink PPP Support Overview

Load balancing operates at Layer 2 or Layer 3 (the network layer) of the Open System Interconnection (OSI) reference model. Layer 3 load balancing is independent of any link-layer technologies. The ATM Multilink Point-to-Point Protocol (PPP) Support on Multiple VCs feature implements load balancing at Layer 2 and depends on having MLP enabled at the link layer.

The ATM MLP functionality keeps track of packet sequencing, and this functionality buffers any packets that arrive early. With this ability, ATM MLP preserves packet order across the entire bundle.

In addition to MLP, low latency queueing (LLQ) and class-based weighted fair queueing (CBWFQ) are used to prioritize and differentiate the voice and data packets. LLQ and CBWFQ help to ensure that the voice and data traffic receive the proper quality of service (QoS) treatment (such as the correct priority queue assignment) when the voice and data traffic are transmitted.

For more information about LLQ and CBWFQ, see the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Benefits of ATM Multilink PPP Support

Facilitates More Efficient Traffic Load Balancing

The ATM Multilink PPP Support on Multiple VCs feature supports the transport of real-time (voice) and other (data) traffic on Frame Relay and ATM VCs.

How to Configure ATM Multilink PPP Support

Defining the Service Policy Using the MQC

Perform this task to define the service policy using the MQC. The MQC allows you to create class maps and define service policies. Service policies are used to create classes and set match criteria for classifying traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all**| **match-any**]
4. **match ip precedence** *ip-precedence-value* [*ip-precedence-value ip-precedence-value ip-precedence-value*]
5. **exit**
6. **policy-map** *policy-name*
7. **class-map** *class-map-name* [**match-all**| **match-any**
8. **bandwidth** {*bandwidth-kbps* | **percent** *percent*}
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-map-name* [**match-all**| **match-any**] **Example:** `Router(config)# class-map class1`	Specifies the name of the class map to be created and enters class-map configuration mode. If match-all or match-any value is not specified, traffic must match all the match criteria to be classified as part of the class map.
Step 4	**match ip precedence** *ip-precedence-value* [*ip-precedence-value ip-precedence-value ip-precedence-value*] **Example:** `Router(config-cmap)# match ip precedence 3 2 4`	Identifies IP precedence values as match criteria.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.
Step 6	**policy-map** *policy-name* **Example:** `Router(config)# policy-map policy1`	Specifies the name of the policy map to be created and enters policy-map configuration mode.
Step 7	**class-map** *class-map-name* [**match-all**| **match-any** **Example:** `Router(config-pmp)# class class2`	Classifies traffic based on the class map specified and enters policy-map class configuration mode.
Step 8	**bandwidth** {*bandwidth-kbps* | **percent** *percent*} **Example:** `Router (config-pmap-c)# bandwidth 45`	Specifies a minimum bandwidth guarantee to a traffic class in periods of congestion. • A minimum bandwidth guarantee can be specified in kbps or by a percentage of the overall available bandwidth.
Step 9	**end** **Example:** `Router(config-pmp)# end`	Exits class-map configuration mode.

Defining a Multilink MLP Bundle Interface

Perform this task to define a multilink MLP bundle interface. The purpose of a multilink bundle interface is to combine more than one permanent virtual circuit (PVC). All configurations for PPP over ATM links are placed into virtual templates, and the bundle parameters are placed into the multilink bundle.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **load-interval** *seconds*
6. **no cdp enable**
7. **service-policy output** *policy-name*
8. **ppp multilink**
9. **ppp multilink fragment disable**
10. **ppp multilink group** *group-number*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface multilink 34`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 209.165.201.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**load-interval** *seconds* **Example:** `Router(config-if)# load-interval 60`	Changes the length of time for which data is used to compute load statistics.

	Command or Action	Purpose
Step 6	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	Disables Cisco Discovery Protocol (CDP) on an interface.
Step 7	**service-policy output** *policy-name* **Example:** `Router(config-if)# service-policy output policy1`	Attaches the specified policy map to the output interface.
Step 8	**ppp multilink** **Example:** `Router(config-if)# ppp multilink`	Enables MLP on an interface.
Step 9	**ppp multilink fragment disable** **Example:** `Router(config-if)# ppp multilink fragment disable`	Disables packet fragmentation.
Step 10	**ppp multilink group** *group-number* **Example:** `Router(config-if)# ppp multilink group 54`	Restricts a physical link to joining only a designated multilink-group interface.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Defining the Virtual Templates for Member Links

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **load-interval** *seconds*
6. **ppp multilink**
7. **ppp multilink group** *group-number*
8. **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** *type number* **Example:** `Device(config)# interface multilink 34`	Configures an interface type and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes existing IP addresses or disables IP processing.
Step 5	**load-interval** *seconds* **Example:** `Device(config-if)# load-interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**ppp multilink** **Example:** `Device(config-if)# ppp multilink`	Enables MLP on the interface.
Step 7	**ppp multilink group** *group-number* **Example:** `Device(config-if)# ppp multilink-group 44`	Restricts a physical link to joining only a designated multilink-group interface.

Step 8	**end**
	Example:
	`Device(config-if)#`
	`end`
		Exits interface configuration mode.

Defining the PVCs and Bundling Member Links

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot* **/0**
   -
   -
   - **interface atm** *slot* / *port*
4. **no ip address**
5. **load interval** *seconds*
6. **atm ilmi-keepalive** [*seconds* [*retry*[*seconds*]]]
7. **pvc** [*name*] *vpi/vci*
8. **vbr-nrt** *output-pcr output-scr* [*output-mbs*]
9. **tx-ring-limit** *ring-limit*
10. **protocol ppp virtual-template** *number*
11. **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	Do one of the following:
	• **interface atm** *slot* **/0**
	•
	•
	• **interface atm** *slot* / *port*
	Example:
	`Device(config)# interface atm 2/0`
	Example:
	`or`
	Example:
		Specifies the ATM interface type and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface atm 2/1`	
Step 4	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes an IP address or disables IP processing.
Step 5	**load interval** *seconds* **Example:** `Device(config-if)# load interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**atm ilmi-keepalive** [*seconds* [*retry*[*seconds*]]] **Example:** `Device(config-if)# atm ilmi-keepalive`	Enables Interim Local Management Interface (ILMI) keepalives.
Step 7	**pvc** [*name*] *vpi/vci* **Example:** `Device(config-if)# pvc pvc1 0/56`	Creates an ATM PVC. Enters interface-ATM-VC configuration mode.
Step 8	**vbr-nrt** *output-pcr output-scr* [*output-mbs*] **Example:** `Device(config-if-atm-vc)# vbr-nrt 45 4 45`	Configures the variable bit rate (VBR)-non real time (NRT) QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size.
Step 9	**tx-ring-limit** *ring-limit* **Example:** `Device(config-if-atm-vc)# tx-ring-limit 3`	Limits the number of particles or packets that can be used on a transmission ring on an interface. • Use this command to tune the transmission ring to assign most of the packets to the Layer 3 queues.
Step 10	**protocol ppp virtual-template** *number* **Example:** `Device(config-if-atm-vc)# protocol ppp virtual-template 34`	Specifies that PPP is established over the ATM PVC using the configuration from the specified virtual template and enters interface configuration mode.
Step 11	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode.

Verifying ATM Multilink PPP Support

Perform this task to display information about ATM Multilink PPP Support on Multiple VCs:

SUMMARY STEPS

1. **enable**
2. **show atm pvc**
3. **show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]]
4. **show interfaces**
5. **show policy-map**
6. **show ppp multilink**
7. **show queueing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** **Example:** `Device# show atm pvc`	Displays all ATM PVCs and traffic information.
Step 3	**show frame-relay pvc** [[**interface** *interface*] [*dlci*] [**64-bit**]	**summary** [**all**]] **Example:** `Device# show frame-relay pvc 16`	Displays statistics about PVCs for Frame Relay interfaces.
Step 4	**show interfaces** **Example:** `Device# show interfaces`	Displays interleaving statistics. • Interleaving data is displayed only if interleaving occurs.
Step 5	**show policy-map** **Example:** `Device# show policy-map`	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
Step 6	**show ppp multilink** **Example:** `Device# show ppp multilink`	Displays bundle information for the MLP bundles and their PPP links in the Device.
Step 7	**show queueing** **Example:** `Device# show queueing`	Lists all or selected configured queueing strategies.

Monitoring ATM Multilink PPP Support

SUMMARY STEPS

1. **enable**
2. **debug atm errors**
3. **debug atm events**
4. **debug ppp error**
5. **debug ppp multilink events**
6. **debug voice rtp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug atm errors** **Example:** `Device# debug atm errors`	Displays ATM errors.
Step 3	**debug atm events** **Example:** `Device# debug atm events`	Displays ATM events.
Step 4	**debug ppp error** **Example:** `Device# debug ppp error`	Displays information on traffic and exchanges in an internetwork implementing the PPP.
Step 5	**debug ppp multilink events** **Example:** `Device# debug ppp multilink events`	Displays information about events affecting multilink groups.
Step 6	**debug voice rtp** **Example:** `Device# debug voice RTP`	Displays information about the interleaving of voice and data packets. • The debug voice RTP command has memory overhead and should not be used when memory is scarce or when traffic is very high.

Configuration Examples for ATM Multilink PPP Support

Defining the Service Policy Using MQC Example

The following example shows how to configure a service policy using the MQC:

```
Device> enable
Device# configure terminal
Device(config)# class-map match-all DATA
Device(config-cmap)# match ip precedence 0
Device(config-cmap)# class-map match-all VOICE
Device(config-cmap)# match access-group 100
Device(config-cmap)# policy-map CISCO
Device(config-pmap)# class VOICE
Device(config-pmap-c)# priority percent 70
Device(config-pmap-c)# class DATA
Device(config-pmap-c)# bandwidth percent 5
Device(config-pmap-c)# access-list 100 permit udp any any precedence critical
```

Defining a Multilink MLP Bundle Interface Example

The following example shows how to define a multilink bundle for the mulitilink interface:

```
Device> enable
Device# configure terminal
Device(config)# interface Multilink1
Device(config-if)# ip address 10.2.1.1 255.0.0.0
Device(config-if)# load-interval 30
Device(config-if)# no cdp enable
Device(config-if)# service-policy output CISCO
Device(config-if)# ppp multilink fragment disable
Device(config-if)# ppp multilink group 1
```

Defining Virtual Templates for Member Links Example

The following example shows how to define virtual templates for member links:

```
Device> enable
Device# configure terminal
Device(config)# interface Virtual-Template1
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# ppp multilink
Device(config-if)# ppp multilink group 1
Device(config-if)# interface Virtual-Template2
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# ppp multilink
Device(config-if)# ppp multilink group 1
```

Defining PVCs and Bundling Member Links Example

The following example shows how to define and configure PVCs as bundle members:

```
Device> enable
Device# configure terminal
Device(config)# interface atm 6/0
Device(config-if)# no ip address
Device(config-if)# load-interval 30
Device(config-if)# atm ilmi-keepalive
Device(config-if)# pvc 0/34

Device(config-if-atm-vc)# vbr-nrt 1536 1536
Device(config-if-atm-vc)# tx-ring-limit 5
Device(config-if-atm-vc)# protocol ppp Virtual-Template1
Device(config-if-atm-vc)# pvc 0/35

Device(config-if-atm-vc)# vbr-nrt 800 800
Device(config-if-atm-vc)# tx-ring-limit 3
Device(config-if-atm-vc)# protocol ppp Virtual-Template2
Device(config-if-atm-vc)# pvc 0/36
Device(config-if-atm-vc)# vbr-nrt 800 400 94
Device(config-if-atm-vc)# tx-ring-limit 5
Device(config-if-atm-vc)# protocol ppp Virtual-Template1
Device(config-if-atm-vc)# pvc 0/37
Device(config-if-atm-vc)# vbr-nrt 800 800
Device(config-if-atm-vc)# tx-ring-limit 3
Device(config-if-atm-vc)# protocol ppp Virtual-Template2
Device(config-if-atm-vc)# end
```

Additional References for ATM Multilink PPP Support on Multiple VCs

The following sections provide references related to the ATM Multilink PPP Support on Multiple VCs feature.

Related Documents

Related Topic	Document Title
QoS configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*
QoS commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
WAN configuration tasks	*Cisco IOS Wide-Area Networking Configuration Guide*
WAN commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Wide-Area Networking Command Reference*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1990	*The PPP Multilink Protocol (MP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ATM Multilink PPP Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 3: Feature Information for ATM Multilink PPP Support on Multiple VCs

Feature Name	Releases	Feature Information
ATM Multilink PPP Support on Multiple VCs	12.2(28)SB 12.2(33)SRE	The ATM Multilink PPP Support on Multiple VCs feature facilitates traffic load balancing on high-speed virtual circuits, using MLP over Frame Relay and ATM. It facilitates traffic load balancing by using MLP to combine packet datagrams on high-speed VCs, as a means for transporting both the voice and data traffic more efficiently.

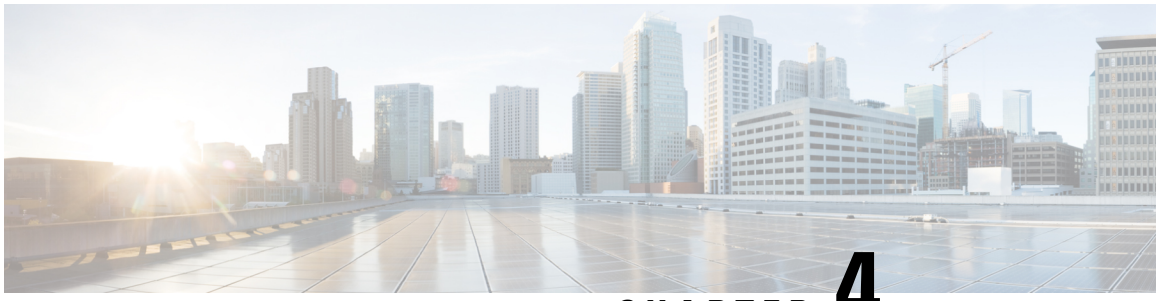
Glossary

LFI --link fragmentation and interleaving. Method of fragmenting large packets and then queueing the fragments between small packets.

MLP --multilink PPP.

QoS --quality of service.

VC --virtual circuit.



CHAPTER 4

ATM OAM Ping

The ATM OAM Ping feature sends an ATM Operation, Administration, and Maintenance (OAM) packet to confirm the connectivity of a specific permanent virtual circuit (PVC). The status of the PVC is displayed when a response to the OAM packet is received. The ATM OAM Ping feature allows the network administrator to verify PVC integrity and facilitates ATM network troubleshooting.

Prerequisites for the ATM OAM Ping Feature

A PVC corresponding to the virtual path identifier (VPI) and virtual channel identifier (VCI) values entered with the **ping** command should already exist.

Restrictions for the ATM OAM Ping Feature

The ATM OAM Ping feature does not support pings based on the following criteria:

- Network service access point (NSAP) addresses
- Multiple-hop loopbacks
- Loopback location identification

Information About the ATM OAM Ping Feature

Benefits of the ATM OAM Ping Feature

The ATM OAM Ping feature modifies the **ping**command, which can be used to send an OAM packet to verify PVC connectivity. The status of the PVC is displayed when a response to the OAM packet is received. This is a common method for testing the accessibility of devices.

The **ping atm interface atm** command provides two ATM OAM ping options:

- End loopback--Verifies end-to-end PVC integrity.
- Segment loopback--Verifies PVC integrity to the immediate neighboring ATM device.

The **ping atm interface atm** command is used to determine the following:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

The simpler **ping** command provides an interactive mode for testing ATM network connectivity. The **ping** command first sends an OAM command loopback cell to the destination and then waits for an OAM response loopback cell. The ping is successful only when the following criteria are met:

- The OAM command loopback cell reaches the destination.
- The destination is able to send an OAM loopback response cell back to the source within a predetermined time called a *timeout* . The default value of the timeout is 2 seconds on Cisco routers.

How to Use the ATM OAM Ping Feature

Testing Network Connectivity Using Ping in Normal Mode

Perform this task to test the network connectivity by using the **ping atm interface atm** command in normal mode; that is, by entering all values for the **ping** test on the command line.

SUMMARY STEPS

1. **enable**
2. **ping atm interface atm** *interface-number vpi-value* [*vci-value* [**end-loopback**[*repeat* [*timeout*]]| **seg-loopback** [*repeat* [*timeout*]]]]

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.

Step 2	**ping atm interface atm** *interface-number vpi-value* [*vci-value* [**end-loopback**[*repeat* [*timeout*]]| **seg-loopback** [*repeat* [*timeout*]]]]
	Example:
	`ping atm interface atm 1/1/0.100 0 500`
	Example:
	`end-loopback 1 2`
	Example:
		Displays a response to confirm the connectivity of a specific PVC for the ASR 1000 series router.
		• **atm** *interface-number* --ATM interface name.
		• *vpi-value* --Virtual path identifier. Range: 0 to 255.
		• *vci-value* --Virtual channel identifier. Range: 0 to 65535.
		• **end-loopback** --Sends ATM end loopback cells. This is the default.
		• **seg-loopback** --Sends ATM segment loopback cells.
		• *repeat* --Number of ping packets that are sent to the destination. Range: 1 to 1000. Default: 5.
		• *timeout* --Timeout interval, in seconds. Range: 1 to 30. Default: 2.

Testing Network Connectivity Using Ping in Interactive Mode

Perform this task to test network connectivity by using the **ping** command; that is, by providing values for the **ping** test by typing the value after the prompts displayed and pressing the **Enter** key. Press the **Enter** key without supplying a value to use the default.

SUMMARY STEPS

1. **enable**
2. **ping**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**ping** **Example:** `Router# ping`	Displays a response to confirm the connectivity of a specific PVC.

Terminating a Ping Session

To terminate a ping session, type the escape sequence--by default, Ctrl-Shift-6.

Configuration Examples for ATM OAM Ping

Verifying the Connectivity of a Specific PVC Example

The following example verifies the connectivity of a specific PVC by sending an ATM OAM packet and confirms the connectivity when it is successful:

```
Router# show atm pvc 10/100
ATM1/1/0.100: VCD: 3, VPI: 10, VCI: 100
UBR, PeakRate: 100000 (235850 cps)
AAL5-LLC/SNAP, etype:0x0, Flags: 0x40, VCmode: 0x0, Encapsize: 12
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
Last cell looped No
Loop detect state 0, Last cell looped 0, OAM Retries 0, Loop Retries 0
OAM VC Status: Not Managed
ILMI VC status: Not Managed
InARP frequency: 15 minutes(s)
Transmit priority 3
InPkts: 78310, OutPkts: 78310, InBytes: 218651435, OutBytes: 218651435
InPRoc: 0, OutPRoc: 16, Broadcasts: 15
InFast: 0, OutFast: 0, InAS: 78310, OutAS: 78281
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 315
F5 InEndloop: 310, F5 InSegloop: 5, F5 InAIS: 0, F5 InRDI: 0
OAM cells sent: 315
F5 OutEndloop: 310, F5 OutSegloop: 5, F5 OutAIS: 0, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
VC 10/100 doesn't exist on 2 of 3 ATM interface(s)
Router#
```

Normal Mode ping atm interface atm Command Example

The following example shows sample output for the **ping atm interface atm**command in normal mode:

```
Router# ping atm interface atm1/1/0.1 500
Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/16/52 ms
Router# ping atm interface atm1/1/0.1 0 500 seg-loopback
Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router# ping atm interface atm1/1/0.1 0 500 end-loopback 100 25
Type escape sequence to abort.
```

```
Sending 100, 53-byte end-to-end OAM echoes, timeout is 25 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/13/180 ms
Router# ping atm interface atm1/1/0.1 0 500 seg-loopback 50 20
Type escape sequence to abort.
Sending 50, 53-byte segment OAM echoes, timeout is 20 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/1/4 ms
Router# show atm pvc 10/100

ATM1/1/0.100: VCD: 3, VPI: 10, VCI: 100
UBR, PeakRate: 100000 (235850 cps)
AAL5-LLC/SNAP, etype:0x0, Flags: 0x40, VCmode: 0x0, Encapsize: 12
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Received
Last cell looped No
Loop detect state 0, Last cell looped 0, OAM Retries 0, Loop Retries 0
OAM VC Status: Verified
ILMI VC status: Not Managed
VC is managed by OAM.
InARP frequency: 15 minutes(s)
Transmit priority 3
InPkts: 78310, OutPkts: 78310, InBytes: 218651435, OutBytes: 218651435
InPRoc: 0, OutPRoc: 16, Broadcasts: 15
InFast: 0, OutFast: 0, InAS: 78310, OutAS: 78281
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 331
F5 InEndloop: 326, F5 InSegloop: 5, F5 InAIS: 0, F5 InRDI: 0
OAM cells sent: 331
F5 OutEndloop: 326, F5 OutSegloop: 5, F5 OutAIS: 0, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
VC 10/100 doesn't exist on 2 of 3 ATM interface(s)
Router#
```

Interactive ping Command Example

The following is sample output for the **ping**command in the interactive mode:

```
router# ping

Protocol [ip]: atm
ATM Interface: atm1/1/0.100
VPI value [0]: 10
VCI value [1]: 100
Loopback - End(0), Segment(1) [0]:
Repeat Count [5]:
Timeout [2]:
Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
```

Additional References

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*
ATM Overview	"Overview of the ATM SPAs"
Configuring ATM OAM traffic reduction	"ATM OAM Traffic Reduction"
Detecting failures when using OAM cells and PVC management	"Troubleshooting PVC Failures When Using OAM Cells and PVC Management"

Standards

Standard	Title
ITU-T Specification I.610 (ITU-T specification for B-ISDN operation and maintenance principles and functions).	I.610 Series I: Integrated Services Digital Network Maintenance principles

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

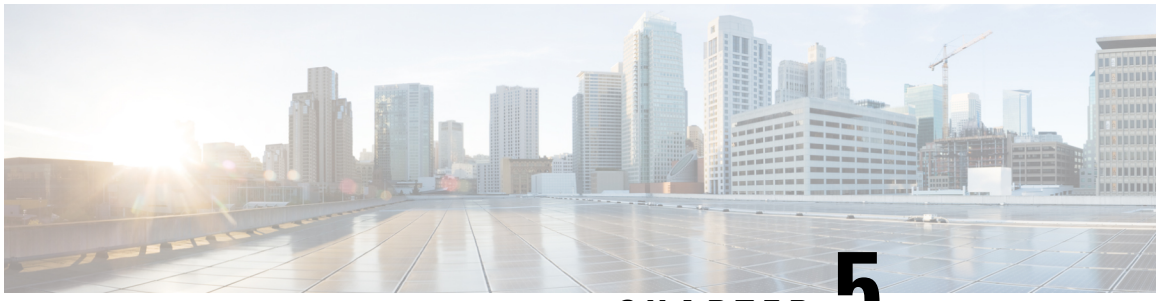
Feature Information for ATM OAM Ping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 4: Feature Information for ATM OAM Ping

Feature Name	Releases	Feature Information
ATM OAM Ping	Cisco IOS XE Release 2.3	The ATM OAM Ping feature sends an ATM OAM packet to confirm the connectivity of a specific PVC. The status of the PVC is displayed when a response to the OAM packet is received. The ATM OAM Ping feature allows the network administrator to verify PVC integrity and facilitates ATM network troubleshooting. The following command was introduced or modified: **ping atm interface atm**.



CHAPTER 5

ATM OAM Traffic Reduction

The ATM OAM Traffic Reduction feature is a mechanism for reducing overhead when loopback cells are being used for fault detection in bidirectional virtual circuits (VCs) over ATM.

Prerequisites for ATM OAM Traffic Reduction

The Operations and Maintenance (OAM) loopback cells described in this document are defined in International Telecommunication Union (ITU) specification *I.610 SERIES I: INTEGRATED SERVICES DIGITAL NETWORK,Maintenance principles* , and understanding this specification is requisite to understanding the ATM OAM Traffic Reduction feature.

Restrictions for ATM OAM Traffic Reduction

- This feature supports only permanent virtual circuits (PVCs) for F5 END_TO_END OAM loopback cells. This feature is not applicable for F4 OAM cells, AIS/RDI cells, or F5 SEGMENT OAM loopback cells.
- This feature breaks OAM loopback functionality when there is a unidirectional breakage and when retry frequency is configured to be the same as the F5 OAM loopback frequency.

Information About ATM OAM Traffic Reduction

OAM Traffic Flow

The OAM management portion of a PVC sends OAM loopback cells at periodic intervals. When OAM management is enabled at both ends of the PVC, the cells are transmitted and looped back at both ends. This transmission is redundant, because the OAM cells travel through the same physical circuit twice.

In the figure below, assume PVCs are configured between router R1 and router R2 , and that OAM management is enabled on both ends of the PVC. Router R1, upon receiving OAM command cells from router R2, can stop its own OAM command cell transmission and can manage the link on the basis of incoming OAM command cells. Router R1 can reinitiate OAM command cell transmission upon discovering the absence of command cells from router R2.

Figure 4: ATM OAM Traffic Flow

When router R1 detects the first OAM command cell from router R2, time stamp T1 is noted. When the next OAM command cell is detected, time stamp T2 is noted. The interval T1 minus T2 provides the OAM the loopback frequency of router R2. The average value of this interval is taken by measuring it a random number of times. (The interval needs to be taken a random number of times to avoid a race condition that *might* happen when routers R1 and R2 implement this algorithm and the frequency is the same.)

At the end of the random time period, router R1 stops sending OAM command cells and starts the OAM traffic monitoring timer. This timer in router R1 checks for a change in interval frequency in router R2. If there is a change, the traffic monitoring timer is stopped and the VC goes into Retry mode and checks whether the link is still up. In Retry mode, OAM command loopback cells are transmitted at an interval of one per second for 3 seconds. If router R1 does not receive a response to the command cell, the link is changed to the Down state.

Note If ATM OAM traffic reduction is enabled on routers R1 and R2, then because of the random nature of the traffic reduction algorithm, either router can initiate OAM command cells and the other router will have to listen to the incoming OAM command cells. If this feature is enabled on only one router (R1, for example), then the frequency of that router must be greater than or equal to the interval frequency set in the other router (R2) in order for router R1 to stop sending OAM command cells. The ATM OAM Traffic Reduction feature is enabled by the **oam-pvc** command. When the **optimum** keyword is enabled, and when a change in the interval frequency of router R2 is detected, the VC initiates an OAM command cell from router R1 and does not go into the Retry mode immediately. If no response is obtained, the VC goes into the Retry mode and follows the OAM Retry procedure.

How to Configure ATM OAM Traffic Reduction

Configuring ATM OAM Traffic Reduction on an ATM Interface

To configure ATM OAM traffic reduction on an ATM interface, use the following commands .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* **.** *subinterface-number*
4. **pvc** *vpi* **/** *vci*
5. **oam-pvc** [*frequency* | **manage** [*frequency* [**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**]]]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* **.** *subinterface-number* **Example:** `Router(config)# interface atm 1/1/1.100`	Configures an ATM interface type and enters interface configuration mode.
Step 4	**pvc** *vpi* **/** *vci* **Example:** `Router(config-if)# pvc 0/100`	Assigns a name to an ATM PVC and enters ATM VC configuration mode.
Step 5	**oam-pvc** [*frequency* | **manage** [*frequency* [**auto-detect** [**optimum**] | **keep-vc-up** [**seg aisrdi failure**] | **loop-detection**]]] **Example:** `Router(config-if-atm-vc)# oam-pvc manage auto-detect optimum`	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or VC class, including the ATM OAM Traffic Reduction feature. • **auto-detect** --Initiates auto-detection of peer OAM command cells.

	Command or Action	Purpose
		• **optimum** --Configures an optimum mode so that when the traffic monitoring timer expires, the PVC sends an OAM command cell at the locally configured frequency instead of going into Retry mode immediately. If there is no response, the PVC goes into Retry mode.
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits the configuration mode. • Enter the **exit** command for each command mode to exit.

Configuring ATM OAM Traffic Reduction on a VC Class

To configure ATM OAM traffic reduction on a VC class, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **oam-pvc** [*frequency* | **manage** [*frequency* [**auto-detect** [**optimum**] | **loop-detection**]]]
5. **exit**
6. **interface atm** *interface-number* **.** *subinterface-number*
7. **class-int** *vc-class-name*
8. **pvc** *vpi* **/** *vci*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm word`	Creates a VC class to an ATM VC bundle member.

	Command or Action	Purpose
Step 4	**oam-pvc** [*frequency* | **manage** [*frequency* [**auto-detect** [**optimum**] | **loop-detection**]]] **Example:** `Router(config-vc-class)# oam-pvc manage auto-detect optimum`	Enables end-to-end F5 OAM loopback cell generation and OAM management for an ATM PVC or VC class, including the ATM OAM Traffic Reduction feature. • **auto-detect** --Initiates autodetection of peer OAM command cells. • **optimum** --Configures an optimum mode so that when the traffic monitoring timer expires, the PVC sends an OAM command cell at the locally configured frequency instead of going into Retry mode. If there is no response, the PVC goes into Retry mode.
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Exits the vc-class mode.
Step 6	**interface atm** *interface-number* **.** *subinterface-number* **Example:** `Router(config)# interface atm 1/1/2.100`	Configures an ATM interface and enters interface configuration mode.
Step 7	**class-int** *vc-class-name* **Example:** `Router(config-if)# class-int test`	Assigns a VC class to an ATM main interface.
Step 8	**pvc** *vpi* **/** *vci* **Example:** `Router(config-if)# pvc 0/100`	Creates an ATM PVC and attaches it to the designated network virtual path identifier (VPI) and virtual channel interface (VCI). In this case, more than one PVC is created.

Step 9	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)# exit`
		Ends the configuration mode.
		• Enter the **exit** command for each command mode to exit.

Verifying ATM OAM Traffic Reduction

To verify that the ATM OAM Traffic Reduction feature is working, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show atm oam auto-detect** [**atm** *interface-number* **.** *subinterface-number*]
3. **show atm pvc** [**interface atm** *type number*[*vpi* / *vci* | *vci* | *word*] *vpi* / *vci* | *vci* | *word*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm oam auto-detect** [**atm** *interface-number* **.** *subinterface-number*] **Example:** `Router# show atm oam auto-detect atm 1/1/2.100`	(Optional) Displays the state of the OAM cells when the ATM OAM traffic reduction is enabled. • The **show atm oam auto-detect** command reports the number of VCs in autodetection mode and in OAM loopback mode.
Step 3	**show atm pvc** [**interface atm** *type number*[*vpi* / *vci* | *vci* | *word*] *vpi* / *vci* | *vci* | *word*] **Example:** `Router# show atm pvc`	(Optional) Displays ATM PVCs and traffic reduction information. The **show atm pvc** command reports the OAM autodetect state, the OAM peer frequency, and the time the last OAM command cell was received.

Configuration Examples for ATM OAM Traffic Reduction

ATM OAM Traffic Reduction on an ATM Interface Example

The following example enables ATM OAM traffic reduction on an ATM interface:

```
interface ATM1/1/1.100 point-to-point
 ip address 60.1.2.1 255.255.255.0
 no atm enable-ilmi-trap
 pvc 11/111
  oam-pvc manage auto-detect optimum
  encapsulation aal5snap
```

ATM OAM Traffic Reduction on a VC Class Example

The following example enables ATM OAM traffic reduction using a VC class:

```
vc-class atm oam-tests
 oam-pvc manage auto-detect optimum
interface ATM1/1/2.100 point-to-point
 ip address 60.1.3.1 255.255.255.0
 class-int oam-tests
 no atm enable-ilmi-trap
 pvc 12/222
  encapsulation aal5snap
```

Verify ATM OAM Traffic Reduction Example

In the following examples, the output is displayed for each command in the task.

Sample Output for the show atm oam auto-detect Command

The following is sample output from the **show atm oam auto-detect** command:

```
Router# show atm oam auto-detect atm 1/1/2.100

ATM OAM Auto Detect statistics on ATM1/1/2
Auto Detection statistics:
ATM OAM AUTO DETECT INIT : 1
ATM OAM SENDING MONITORING : 0
ATM OAM MONITORING : 0
OAM Loopback statistics:
 DownRetry : 0
 UpRetry : 0
 Verified : 1
 Not Verified : 0
 Verified and Not Monitoring: 1
Router#
```

Sample Output for the show atm pvc Command

The following is sample output from the **show atm pvc** command with ATM OAM traffic reduction enabled:

```
Router# show atm pvc 12/222

ATM1/1/2.100: VCD: 1, VPI: 12, VCI: 222
UBR, PeakRate: 149760 (353208 cps)
AAL5-LLC/SNAP, etype:0x0, Flags: 0x1840, VCmode: 0x0, Encapsize: 12
OAM frequency: 10 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Received
Last cell looped No
Loop detect state 0, Last cell looped 0, OAM Retries 0, Loop Retries 0
OAM VC Status: Verified
OAM Auto Detect state: ATM OAM AUTO DETECT INIT
OAM PEER frequency: 0 second(s)
```

Additional References for ATM OAM Traffic Reduction

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

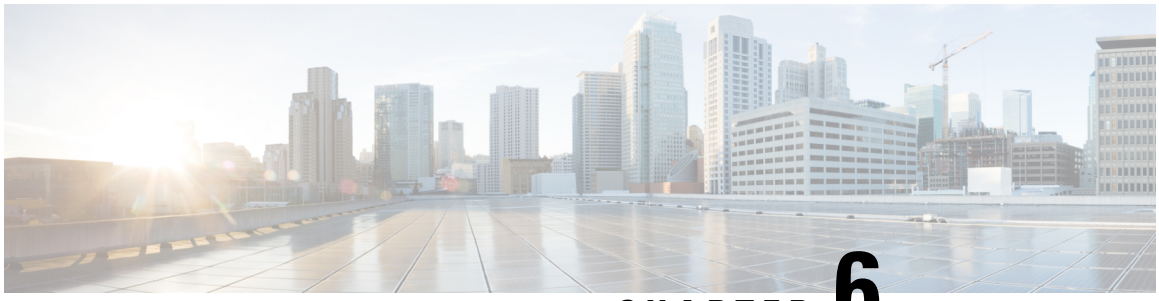
Feature Information for ATM OAM Traffic Reduction

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 5: Feature Information for ATM OAM Traffic Reduction

Feature Name	Releases	Feature Information
ATM OAM Traffic Reduction	Cisco IOS XE Release 2.3S Cisco IOS XE Release 3.14S	The ATM OAM Traffic Reduction feature is a mechanism for reducing overhead when loopback cells are being used for fault detection in bidirectional virtual circuits (VCs) over ATM. In Cisco IOS Release XE 3.14S, support for the ATM OAM Traffic Reduction feature was added on the 4451-X Integrated Services Router. The following commands were introduced or modified: **oam-pvc show atm oam auto-detect show atm pvc**



CHAPTER 6

Local Template-Based ATM PVC Provisioning

The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. ATM PVC autoprovisioning can be configured on a PVC, an ATM PVC range, or a VC class. If a VC class configured with ATM PVC autoprovisioning is assigned to an interface, all the PVCs on that interface will be autoprovisioned; this configuration is sometimes referred to as an *infinite range*.

Restrictions for Local Template-Based ATM Provisioning

The number of PVCs that can be established on an interface that is configured as an infinite range is limited to the maximum number of VCs that the platform can support.

Information About Local Template-Based ATM Provisioning

Autoprovisioned ATM PVCs are not created until there is activity on the virtual path identifier (VPI)/virtual channel identifier (VCI) pair. When the interface is disabled and reenabled using the **shutdown** and **no shutdown** commands, autoprovisioned PVCs that are part of a PVC range or infinite range are removed upon shutdown and are not reestablished until the first incoming packet triggers PVC creation. During router reload, autoprovisioned PVCs are created when there is activity on the connection.

The total number of VCs that can be configured on an ATM port adapter is limited by the capacity of the port adapter. In cases of ATM link oversubscription, where a PVC range or infinite range is configured to provision more PVCs than the port adapter allows, the PVCs can be configured with a timeout so that they can be dynamically brought down as needed. When the timeout expires, the idle PVCs are removed, allowing the PVC range or infinite range of PVCs to share system resources.

ATM PVC local autoprovisioning supports the following applications: PPP over ATM, ATM routed bridge encapsulation, and routed RFC 1483.

The Local Template-Based ATM Provisioning feature enables ATM PVCs to be created automatically as needed from a local configuration, making the provisioning of large numbers of digital subscriber line (DSL) subscribers easier, faster, and less prone to error.

How to Configure Local Template-Based ATM Provisioning

Configuring ATM PVC Local Autoprovisioning in a VC Class

A VC class configured with ATM PVC autoprovisioning can be assigned to an ATM interface, an ATM PVC, an ATM PVC range, and an ATM PVC with a range.

Note If a VC class that is configured with ATM PVC autoprovisioning is assigned to an ATM interface, all PVCs on the interface will be autoprovisioned.

To enable ATM PVC local autoprovisioning in a VC class, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **create on-demand**
5. **idle-timeout** *seconds* [*minimum-rate*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm auto-pppoe`	Creates a VC class for an ATM PVC, SVC, or ATM interface and enters ATM VC class configuration mode.

	Command or Action	Purpose
Step 4	**create on-demand** **Example:** `Router(config-vc-class)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 5	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-vc-class)# idle-timeout 300 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 6	**end** **Example:** `Router(config-vc-class)# end`	(Optional) Exits the ATM VC class configuration mode and returns to privileged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on a PVC

ATM PVC local autoprovisioning can also be configured on a PVC by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the PVC.

To enable ATM PVC local autoprovisioning on a PVC, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** slot/subslot/port[.subinterface]
4. **atm autovc retry** *interval*
5. **pvc** [*name*] *vpi* / *vci*
6. **create on-demand**
7. **idle-timeout** *seconds* [*minimum-rate*]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface atm** slot/subslot/port[.subinterface] **Example:** `Router(config)# interface atm5/0`	Configures an ATM interface.
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 60`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 1/300`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**create on-demand** **Example:** `Router(config-if-atm-vc)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 7	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-vc)# idle-timeout 300 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 8	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits the ATM virtual circuit configuration mode and returns to privileged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on an ATM PVC Range

ATM PVC local autoprovisioning can also be configured on a range by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the range.

To enable ATM PVC autoprovisioning on an ATM PVC range, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** slot/subslot/port[**.** *subinterface*]
4. **atm autovc retry** *interval*
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
6. **create on-demand**
7. **idle-timeout** *seconds* [*minimum-rate*]

8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** slot/subslot/port[**.** *subinterface*] **Example:** `Router(config)# interface atm5/0`	Configures an ATM interface.
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 60`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-if)# range auto pvc 0/100 1/200`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**create on-demand** **Example:** `Router(config-if-atm-range)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 7	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-range)# idle-timeout 300 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 8	**end** **Example:** `Router(config-if-atm-range)# end`	(Optional) Exits the ATM PVC range configuration mode and returns to privileged EXEC mode.

Configuring ATM PVC Local Autoprovisioning on PVC Within a Range

ATM PVC local autoprovisioning can also be configured on a PVC within a range by assigning a VC class that has been configured with ATM PVC local autoprovisioning to the PVC.

To enable ATM PVC autoprovisioning on a PVC within an ATM PVC range, use the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** slot/subslot/port[**.** *subinterface*]
4. **atm autovc retry** *interval*
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
6. **pvc-in-range** [*pvc-name*] [*vpi* /]*vci*]
7. **create on-demand**
8. **idle-timeout** *seconds* [*minimum-rate*]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** slot/subslot/port[**.** *subinterface*] **Example:** `Router(config)# interface atm5/0`	Configures an ATM interface.
Step 4	**atm autovc retry** *interval* **Example:** `Router(config-if)# atm autovc retry 60`	(Optional) Configures the interval at which the router will repeat the attempt to create autoprovisioned PVCs after a failure of the initial creation attempt.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-if)# range auto pvc 0/100 1/200`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.

	Command or Action	Purpose
Step 6	**pvc-in-range** [*pvc-name*] [*vpi* /]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range 0/101`	Defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.
Step 7	**create on-demand** **Example:** `Router(config-if-atm-range-pvc)# create on-demands`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.
Step 8	**idle-timeout** *seconds* [*minimum-rate*] **Example:** `Router(config-if-atm-range-pvc)# idle-timeout 300 10`	(Optional) Configures the idle timeout parameter for tearing down ATM SVC connections or autoprovisioned ATM PVC connections.
Step 9	**end** **Example:** `Router(config-if-atm-range-pvc)# end`	(Optional) Exits the PVC-in-range configuration mode and returns to privileged EXEC mode.

Verifying ATM PVC Autoprovisioning

To verify that ATM PVC local autoprovisioning is configured and working correctly, perform the tasks in the following steps:

SUMMARY STEPS

1. Enter the **show running-config** command to verify that the configuration is correct.
2. Enter the **show atm pvc** command. PVCs that have been autoprovisioned will have the value "PVC-A" ("A" stands for automatic) in the Type field.
3. Enter the **show atm pvc** command with the *vpi*/*vci* arguments to see if ATM PVC local autoprovisioning is configured on a specific PVC. If ATM PVC local autoprovisioning is configured, the text "VC Auto Creation Enabled: local" will appear in the output.

DETAILED STEPS

Step 1 Enter the **show running-config** command to verify that the configuration is correct.

Step 2 Enter the **show atm pvc** command. PVCs that have been autoprovisioned will have the value "PVC-A" ("A" stands for automatic) in the Type field.

Example:

```
Router# show atm pvc
            VCD /                                       Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
5/0.1       117        0     50   PVC-A   SNAP    UBR  149760                UP
```

```
5/0.1       118        0     51   PVC-A   SNAP    UBR  149760               UP
5/0.1       119        0     52   PVC-A   SNAP    UBR  149760               UP
```

Step 3 Enter the **show atm pvc** command with the *vpi*/*vci* arguments to see if ATM PVC local autoprovisioning is configured on a specific PVC. If ATM PVC local autoprovisioning is configured, the text "VC Auto Creation Enabled: local" will appear in the output.

Example:

```
Router# show atm pvc 0/51
ATM5/0.1: VCD: 118, VPI: 0, VCI: 51
UBR, PeakRate: 149760
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20000C20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minutes(s)
Transmit priority 4
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0, CPIErrors: 0
Out CLP=1 Pkts: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
PPP: Virtual-Access3 from Virtual-Template1
VC Auto Creation Enabled: local
```

Monitoring and Maintaining ATM PVC Local Autoprovisioning

To monitor and maintain ATM PVC autoprovisioning, use one or more of the following commands.

SUMMARY STEPS

1. **enable**
2. **debug atm autovc** {**event** | **error** | **all**}
3. **show atm pvc**
4. **show atm vc**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**debug atm autovc** {**event** | **error** | **all**} **Example:** `Router# debug atm autovc all`	Displays information about autoprovisioned ATM PVC events and errors.
Step 3	**show atm pvc** **Example:** `Router# show atm pvc`	Displays all ATM PVCs and traffic information.
Step 4	**show atm vc** **Example:** `Router# show atm vc`	Displays all ATM PVCs and SVCs and traffic information.

Configuration Examples for Local Template-Based ATM Provisioning

ATM PVC Local Autoprovisioning on an ATM Interface Example

In the following example, local autoprovisioning is enabled on all PVCs on ATM interface 5/0:

```
vc-class atm auto-pppoe
 vbr-nrt 1000 100
 protocol pppoe
 create on-demand
 idle-timeout 300 10
!
interface atm 5/0
 class-int auto-pppoe
 atm autovc retry 10
```

ATM PVC Local Autoprovisioning on a PVC Example

The following example shows the configuration of local autoprovisioning on a PVC:

```
interface atm 5/0
 pvc 1/300
  create on-demand
  idle-timeout 300 10
```

ATM PVC Local Autoprovisioning on an ATM PVC Range Example

The following example shows the configuration of local autoprovisioning on an ATM PVC range called "auto":

```
interface atm 5/0
 range auto pvc 0/100 1/200
  create on-demand
```

ATM PVC Local Autoprovisioning on a PVC Within a Range Example

The following example shows the configuration of local autoprovisioning on a PVC within a PVC range:

```
interface atm 5/0
 range auto pvc 0/100 1/200
  pvc-in-range 0/101
   create on-demand
```

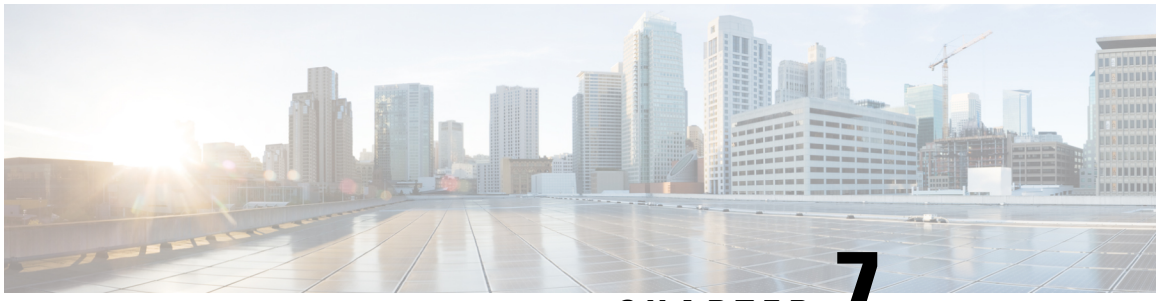
Feature Information for Local Template-Based ATM PVC Provisioning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 6: Feature Information for Local Template-Based ATM PVC Provisioning

Feature Name	Releases	Feature Information
Local Template-Based ATM PVC Provisioning	Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The Local Template-Based ATM Provisioning feature enables ATM permanent virtual circuits (PVCs) to be provisioned automatically as needed from a local configuration. The following commands were introduced or modified: **atm autovc retry, create on-demand, debug atm autovc, idle-timeout.**



CHAPTER 7

ATM PVC Range

In a digital subscriber line (DSL) environment, many applications require the configuration of a large number of ATM permanent virtual circuits (PVCs). The ATM PVC RangeSubinterface Grouping feature enables you to group a number of PVCs together into a PVC *range* in order to configure them all at once.

Restrictions for ATM PVC Range

You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All of the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

Information About Restrictions for ATM PVC Range

For applications that use multipoint subinterfaces, such as PPP over Ethernet and PPP over ATM, the PVC range is on a single multipoint subinterface.

A PVC range is defined by two VPI-VCI pairs. The two virtual path identifiers (VPIs) define a VPI range, and the two virtual channel identifiers (VCIs) define a VCI range. The number of PVCs in the PVC range equals the number of VPIs in the VPI range multiplied by the number of VCIs in the VCI range.

Once the PVC range is defined, you can configure the range by using the existing interface-ATM-VC configuration commands that are also supported in PVC range configuration mode. The **shutdown** PVC range command can be used to deactivate the range without deleting the configuration.

The ATM PVC Range feature also introduces the **pvc-in-range** command, which allows you to explicitly configure an individual PVC within the defined range of PVCs on a multipoint subinterface. The **shutdown** PVC-in-range command allows you to deactivate an individual PVC within a range.

Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All of the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

Benefits of ATM PVC Range

Saving Time

Configuring a range of PVCs is faster than configuring each PVC individually.

Saving NVRAM

A range of PVCs takes up less NVRAM on network service routers than a large number of individually configured PVCs.

Speeding Boot-Up

The parser can parse one configuration command instead of many, thus speeding bootup time.

How to Configure ATM PVC Range

Configuring an ATM PVC Range

Note For point-to-point subinterfaces, subinterface numbering begins with the subinterface on which the PVC range is configured and increases sequentially through the range.

To configure an ATM PVC range, use the following commands beginning in global configuration mode

SUMMARY STEPS

1. Router(config)# **interface atm** *slot/port.subinterface-number* {**point-to-point** | **multipoint**}
2. Router(config-subif)# **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
3. Router(config-if-atm-range)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot/port.subinterface-number* {**point-to-point** | **multipoint**}	Configures an ATM subinterface and enters subinterface configuration mode.
Step 2	Router(config-subif)# **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*	Defines a range of PVCs and enables PVC range configuration mode.

	Command or Action	Purpose
		The number of PVCs in a range can be calculated using the following formula: • number of PVCs = (*end-vpi* - *start-vpi* + 1) x (*end-vci* - *start-vci* +1). • The *start-vpi* argument may be omitted if it is zero. The *end_vpi*argument may be omitted, but if it is omitted, it is assigned the value of *start-vpi*. The *end-vpi* and *end-vci* arguments are always greater than or equal to *start-vpi* and *start-vci*, respectively.
Step 3	Router(config-if-atm-range)# **exit**	Exits PVC range configuration mode.

Deactivating a PVC Range

To deactivate a PVC range, use the following command in PVC range configuration mode:

Command	Purpose
`Router(config-if-atm-range)#` **`shutdown`**	Deactivates a PVC range.

Configuring an Individual PVC Within a PVC Range

To configure an individual PVC within a PVC range on a multipoint subinterface, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface atm** *slot*/*port.subinterface-number* **multipoint**
2. Router(config-subif)# **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
3. Router(config-if-atm-range)# **pvc-in-range** [*pvc-name*] [*vpi*/*vci*]
4. Router(cfg-if-atm-range-pvc)# **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface atm** *slot*/*port.subinterface-number* **multipoint**	Configures an ATM interface.
Step 2	Router(config-subif)# **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*	Defines a range of PVCs and enables PVC range configuration mode.
Step 3	Router(config-if-atm-range)# **pvc-in-range** [*pvc-name*] [*vpi*/*vci*]	Defines an individual PVC within a PVC range, and enables PVC-in-range configuration mode.

	Command or Action	Purpose
Step 4	Router(cfg-if-atm-range-pvc)# **exit**	Exits PVC-in-range configuration mode.

Deactivating an Individual PVC Within a PVC Range

To deactivate an individual PVC within a range, use the following command in PVC-in-range configuration mode:

Command	Purpose
`Router(cfg-if-atm-range-pvc)# shutdown`	Deactivates an individual PVC within a range.

Verifying an ATM PVC Range

To verify ATM PVC range configuration, use the following EXEC command:

Command	Purpose
`Router# show atm pvc [vpi/vci | name | interface atm interface-number]`	Displays ATM PVCs and traffic information.

Configuration Examples for ATM PVC Range

ATM PVC Range on a Multipoint Subinterface Example

In the following example, a PVC range called "range-pppoa-1" is created with a total of 500 PVCs in the range. PVC parameters are configured for the range, including the assignment of a VC class called "classA."

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range-pppoa-1 pvc 100 4/199
Router(config-if-atm-range)# class-range classA
Router(config-if-atm-range)# ubr 1000
Router(config-if-atm-range)# encapsulation aal5snap
Router(config-if-atm-range)# protocol ppp virtual-template 2
```

Individual PVC Within a PVC Range Configuration Example

In the following example, "pvc1" within the PVC range called "range1" is deactivated.

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range1 pvc 100 4/199
Router(config-if-atm-range)# class-range classA
```

```
Router(config-if-atm-range)# pvc-in-range pvc1 3/104
Router(cfg-if-atm-range-pvc)# shutdown
```

Additional References

Related Documents

Related Topic	Document Title
Configuring ATM	"Configuring ATM" chapter in the *Cisco IOS Asynchronous Transfer Mode Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

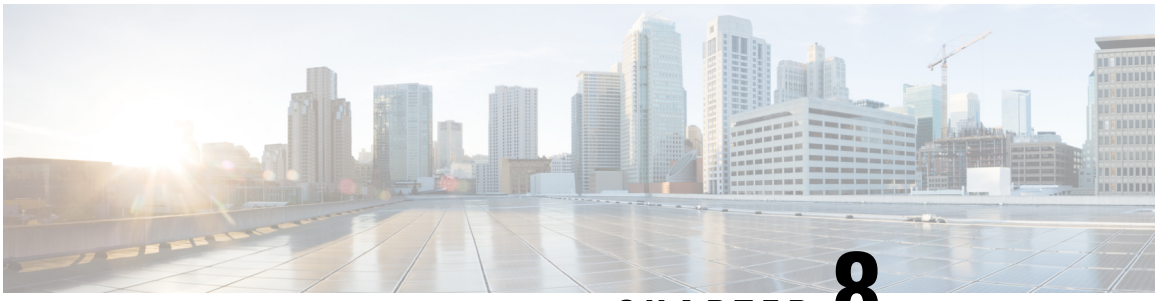
Feature Information for ATM PVC Range

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 7: Feature Information for ATM PVC Range and RBE Subinterface Grouping

Feature Name	Releases	Feature Information
ATM PVC Range	12.1(5)T 12.2(28)SB XE 2.5.0	The ATM PVC Range Subinterface Grouping feature enables you to group a number of PVCs together into a PVC range in order to configure them all at once. In 12.1(5)T, this feature was introduced on the Cisco 7200. The following commands were introduced or modified: **class-range, oam-range, pvc-in-range, range pvc, shutdown(PVC-in-range), shutdown(pvc-range)**.



CHAPTER 8

Configuring ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature provides the ability to send Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) when the PVC state changes and when Operation, Administration and Maintenance (OAM) loopback fails for a PVC. This feature also provides information about the virtual path identifier/virtual channel identifier (VPI/VCI) in the ATM PVC traps.

The ATM OAM AIS-RDI Monitoring feature extends the existing ATM virtual circuit OAM functionality to include monitoring of the Alarm Indication Signal-Remote Defect Indication (AIS-RDI).

Prerequisites for ATM SNMP Trap and OAM Enhancements

Before you enable ATM PVC trap support, you must configure Simple Network Management Protocol (SNMP) support and an IP routing protocol on your router. For more information about configuring SNMP support, refer to the chapter "Configuring SNMP Support" in the *Cisco IOS XE Network Management Configuration Guide*.

To receive PVC failure notification and to allow access to PVC status tables on your router, you must have the Cisco extended ATM PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my compiled in your Network Management System (NMS) application. You can find this MIB at Cisco's MIB website: http://www.cisco.com/go/mibs.

The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps are configured.

Restrictions for ATM SNMP Trap and OAM Enhancements

- Extended ATM PVC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps are configured.
- ATM PVC UP traps are not generated for newly created PVCs. They are generated only for PVCs that go from the DOWN state to the UP state.

Information About ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the SNMP notifications for ATM permanent virtual circuits (PVCs) and to OAM functionality:

- ATM PVC traps will be generated when the operational state of a PVC changes from the DOWN state to the UP state.
- ATM PVC traps will be generated when OAM loopback fails, and the PVC will remain in the UP state, rather than going down.
- The ATM PVC traps are now extended to include virtual path identifier/virtual channel identifier (VPI/VCI) information, the number of state transitions a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

ATM PVC Up Trap

Before the introduction of the ATM SNMP trap and OAM enhancements, the only SNMP notifications for ATM PVCs were the ATM PVC failure traps that were generated when a PVC failed or left the UP operational state. The ATM SNMP trap and OAM enhancements introduce ATM PVC up traps, which are generated when a PVC changes from the DOWN state to the UP state.

ATM PVC OAM Failure Trap

The ATM SNMP trap and OAM enhancements introduce the ATM PVC OAM failure trap. OAM loopback is a mechanism that detects whether a connection is up or down by sending OAM end-to-end loopback command/response cells. An OAM loopback failure indicates that the PVC has lost connectivity. The ATM PVC OAM failure trap is generated when OAM loopback for a PVC fails and is sent at the end of the notification interval.

When OAM loopback for a PVC fails, the PVC is included in the atmStatusChangePVclRangeTable or atmCurrentStatusChangePVclTable and in the ATM PVC OAM failure trap.

Before this feature was introduced, if OAM loopback failed, the PVC was placed in the DOWN state. When the ATM PVC OAM failure trap is enabled, the PVC remains up even if OAM loopback fails, and thus it ensures continuous flow of data.

Note ATM PVC traps are generated at the end of the notification interval. It is possible to generate three types of ATM PVC traps (the ATM PVC failure trap, ATM PVC up trap, and ATM PVC OAM failure trap) at the end of the same notification interval. However, only one type of trap is generated for each PVC.

Extended ATM PVC Traps

The ATM SNMP Trap and OAM Enhancements feature introduces extended ATM PVC traps. The extended traps include VPI/VCI information for affected PVCs, the number of up-to-down and down-to-up state transitions that a PVC goes through in an interval, and the time stamp of the first and the last PVC state transition.

Note Extended ATM PVC traps cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC traps are configured.

ATM PVC High Watermark Trap

The ATM SNMP Trap and OAM Enhancements feature introduces a high watermark trap. A trap is generated when the number of configured PVCs in an interface and related subinterfaces exceeds a preconfigured high watermark threshold. When the number of configured PVCs in an interface and related subinterfaces falls below the high watermark threshold, another trap is generated to indicate that the fault is cleared. A minimum duration between the occurrence of two consecutive high watermark thresholds can also be set.

Supported MIB Objects and Tables

The ATM PVC trap is defined in the ATM PVC trap MIB. The ATM SNMP trap and OAM enhancements introduce the following tables and MIB objects:

- The table atmInterfaceExt2Table displays the status of ATM PVCs and is indexed by ifIndex. This table contains the following objects:
  - atmIntfCurrentlyDownToUpPVcls
  - atmIntfOAMFailedPVcls
  - atmIntfCurrentlyOAMFailingPVcls
- The table atmCurrentStatusChangePVclTable displays information about ATM PVCs that undergo an operational state change and is indexed by ifIndex, atmVclVpi, and atmVclVci. This table contains the following objects:
  - atmPVclStatusTransition
  - atmPVclStatusChangeStart
  - atmPVclStatusChangeEnd
- The table atmStatusChangePVclRangeTable displays information about ATM PVC ranges and is indexed by ifIndex, atmVclVpi, and rangeIndex. This table contains the following objects:

- atmPVclLowerRangeValue
- atmPVclHigherRangeValue
- atmPVclRangeStatusChangeStart
- atmPVclRangeStatusChangeEnd

- The ATM PVC Up Trap "atmIntfPvcUpTrap" contains the following objects:
  - ifIndex
  - atmIntfCurrentlyDownToUpPVcls
- The ATM PVC OAM Failure Trap atmIntfPvcOAMFailureTrap contains the following objects:
  - ifIndex
  - atmIntfOAMFailedPVcls
  - atmIntfCurrentlyOAMFailingPVcls

ATM OAM AIS-RDI Monitoring

The ATM OAM Alarm Indication Signal--Reverse Defect Indication (AIS-RDI) Monitoring feature extends the existing ATM VC OAM functionality to include monitoring of the AIS-RDI. Once the feature is enabled, OAM AIS-RDI is monitored on the VCs. If the number of consecutive OAM AIS-RDI cells received is greater than a configurable number, the VC is brought down. The VC is brought up when there are no OAM AIS-RDI cells received within a configurable interval.

Benefits of Configuring ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements and the ATM OAM AIS-RDI Monitoring features have the following benefits:

- Enables you to use SNMP to detect the recovery of PVCs that are down.
- Enables you to use SNMP to detect when OAM loopback fails for a PVC.
- Keeps the PVC in the UP state when OAM loopback fails to allow continuous flow of data.
- Provides VPI/VCI information in the ATM PVC traps to let you know the PVC that changed operational state or encountered an OAM loopback failure.
- Provides statistics on the number of state transitions that a PVC goes through.
- Provides flexibility to control the status change of a PVC when a faulty condition is detected on a VC and OAM VC-AIS cells are generated.
- Generates a trap to identify if configured PVCs under an interface and related subinterfaces exceed the configured threshold.

How to Configure ATM SNMP Trap and OAM Enhancements

Configuring Extended ATM PVC Trap Support

Perform this task to configure extended ATM PVC trap support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps atm pvc extension** {**up**| **down**| **oam failure**[**aisrdi**| **loopback**]}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps atm pvc extension** {**up**| **down**| **oam failure**[**aisrdi**| **loopback**]} **Example:** `Router(config)# snmp-server enable traps atm pvc extension oam failure loopback`	Enables the sending of extended ATM PVC traps. The keywords are as follows: • **up** --Enables ATM PVC up traps that are generated when a PVC changes from the down state to the up state. • **down** --Enables ATM PVC failure traps that are generated when a PVC changes from the up state to the down state. • **oam failure** --Enables ATM PVC OAM failure traps that are generated when an OAM failure occurs. • **aisrdi** --(optional) Enables AIS/RDI OAM failure traps that are generated when an AIS/RDI OAM failure occurs. • **loopback** --(optional) Enables OAM failure loopback traps that are generated when an OAM loopback failure occurs.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring ATM PVC High Watermark Trap Support

Perform this task to configure ATM PVC high watermark trap support using Remote Monitoring (RMON).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* **.** *subinterface-number* **point-to-point**
4. **no atm enable-ilmi-trap**
5. **exit**
6. **rmon event** *number* **log trap** *community* **owner** *owner-name*
7. **rmon alarm** *number variable interval* **absolute rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] **owner** *owner-name* **interface atm** *slot* / *subslot* / *port* **.** *subinterface-number* **trap**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* **.** *subinterface-number* **point-to-point** **Example:** `Router(config)# interface atm 1/0/0.2 point-to-point`	Configures the ATM interface. The command syntax is as follows: • *slot/subslot/port* --Specifies a (physical) ATM interface (for example, 0/2/0). • **.** *subinterface-number* --Specifies a subinterface number. A dot (.) must be used to separate the interface number from the subinterface number (for example, 0/2/0.1).

	Command or Action	Purpose
		• **point-to-point** --Specifies point-to-point as the interface type for which a subinterface is to be created.
Step 4	**no atm enable-ilmi-trap** **Example:** `Router(config-if)# no atm enable-ilmi-trap`	Does not generate an Integrated Local Management Interface (ILMI) atmfVccChange trap when an ATM interface or subinterface is enabled or shut down.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 6	**rmon event** *number* **log trap** *community* **owner** *owner-name* **Example:** `Router(config)# rmon event 3 log trap public owner Test`	Creates RMON event, which is the prerequisite for generating a trap.
Step 7	**rmon alarm** *number variable interval* **absolute rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] **owner** *owner-name* **interface atm** *slot* / *subslot* / *port* **.** *subinterface-number* **trap** **Example:** `Router(config)# rmon alarm 1 ciscoAtmIfPVCs 4 absolute rising-threshold 5 1 falling-threshold 4 1 owner conf interface Atm3/0 trap`	Generates a trap when the number of configured PVCs in an interface and related subinterfaces exceed a preconfigured high watermark threshold. The **interface** keyword enables RMON to monitor the ciscoAtmIfPVCs object for the specific interface. The **trap**keyword enables RMON to include the interface name in the generated trap.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling OAM Management

When you configure PVC trap support, you must also enable OAM management on the PVC. Perform this task to enable OAM management.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* [**.** *subinterface-number*{**multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci*
5. **oam-pvc manage**

6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* [**.** *subinterface-number*{**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 0/2/0`	Specifies the ATM interface. The command syntax is as follows: • *slot/subslot/port* --Specifies a (physical) ATM interface (for example, 0/2/0). • **.** *subinterface-number* --Specifies a subinterface number. A dot (.) must be used to separate the interface number from the subinterface number (for example, 0/2/0.1). • **multipoint** --Specifies multipoint as the interface type for which a subinterface is to be created. • **point-to-point** --Specifies point-to-point as the interface type for which a subinterface is to be created.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc oam 0/5`	Enables the PVC and enters ATM VC configuration mode.
Step 5	**oam-pvc manage** **Example:** `Router(config-if-atm-vc)# oam-pvc manage`	Enables end-to-end OAM management for an ATM PVC.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM VC configuration mode and returns to priviledged EXEC mode.

Enabling OAM AIS-RDI Monitoring

Perform this task to enable OAM AIS-RDI monitoring on VCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* [**.** *subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci*
5. **oam ais-rdi** [*down-count* [*up-count*]]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* [**.** *subinterface-number* {**multipoint**	**point-to-point**}] **Example:** `Router(config)# interface atm 2/0/0`	Specifies the ATM interface and enters interface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 0/400`	Enables the PVC and enters ATM VC configuration mode.
Step 5	**oam ais-rdi** [*down-count* [*up-count*]] **Example:** `Router(config-if-atm-vc)# oam ais-rdi 1 3`	Configures an ATM PVC to be brought down after a specified number of OAM AIS/RDI cells have been received on the PVC or to be brought up if no OAM AIS/RDI cells have been received in a specified interval.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM VC configuration mode and returns to privileged EXEC mode.

Verifying ATM PVC Traps

To verify the configuration of ATM PVC traps, use the **show running-config** command.

SUMMARY STEPS

1. **show atm vc**

DETAILED STEPS

show atm vc

The following is sample output from the **show atm vc** command:

Example:

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
          VCD /                                              Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
0/2/0        oam           0     5 PVC     SNAP       UBR       0              IN
0/2/0        7             0    10 PVC     SNAP       UBR       0              IN
0/2/0        2             0    40 PVC     SNAP       UBR       0              IN
0/2/0        1             0   100 PVC     SNAP       UBR       0              IN
0/2/0        name          1     1 PVC     SNAP       UBR       0              IN
0/2/0        4             2   200 PVC     SNAP       UBR       0              IN
0/2/0        vpi/vci       3   100 PVC     SNAP       UBR       0              IN
0/2/0        8             4   100 PVC     SNAP       UBR       0              IN
```

Configuration Examples for ATM SNMP Traps and OAM Enhancements

Example Configuring Extended ATM PVC Trap Support

The following example shows the three extended ATM PVC traps enabled on a router. If PVC 0/1 either leaves the up state or down state or encounters an OAM loopback failure, then the host 172.16.61.90 receives SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 0/1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Examples Extended ATM PVC Trap Output

This section contains examples of output for the extended ATM PVC traps.

Extended ATM PVC Failure Trap Output

The following example shows the output for the extended ATM PVC failure trap for PVCs 1/100, 1/102, and 1/103. Note that only one trap is generated for all the PVCs associated with the same interface or subinterface (in contrast to the legacy ATM PVC failure trap that generates a separate trap for each PVC). The VPI/VCI information and timing are located in the objects that are associated with the trap.

```
00:23:56:SNMP:Queuing packet to 1.1.1.1
00:23:56:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 143636
snmpTrapOID.0 = atmIntfPvcFailuresTrap
ifEntry.1.19 = 19
atmIntfPvcFailures.2 = 7
atmIntfCurrentlyFailingPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 140643
atmPVclRangeStatusChangeEnd.19.1.2 = 140698
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 140636
atmPVclStatusChangeEnd.19.1.100 = 140636
00:23:56:SNMP:Packet sent via UDP to 1.1.1.1
```

Extended ATM PVC Up Trap Output

The following example shows the output for the extended ATM PVC up trap for PVCs 1/100, 1/102, and 1/103:

```
00:31:29:SNMP:Queuing packet to 1.1.1.1
00:31:29:SNMP:V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 188990
snmpTrapOID.0 = atmIntfPvcUpTrap
ifEntry.1.19 = 19
atmIntfCurrentlyDownToUpPVcls.2 = 3
atmPVclLowerRangeValue.19.1.2 = 102
atmPVclHigherRangeValue.19.1.2 = 103
atmPVclRangeStatusChangeStart.19.1.2 = 186005
atmPVclRangeStatusChangeEnd.19.1.2 = 186053
atmPVclStatusTransition.19.1.100 = 1
atmPVclStatusChangeStart.19.1.100 = 185990
atmPVclStatusChangeEnd.19.1.100 = 185990
00:31:30:SNMP:Packet sent via UDP to 1.1.1.1
```

Example Enabling OAM AIS-RDI Monitoring

The following example shows how to enable OAM ASI-RDI monitoring in ATM VC configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# interface atm 2/0/0
Router(config-if)# pvc 0/400
Router(config-if-atm-vc)# oam ais-rdi 25 5
Router(config-if-atm-vc)# end
```

The following example shows how to enable OAM ASI-RDI monitoring in ATM VC class configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm vctest
Router(config-vc-class)# oam ais-rdi 14 5
Router(config-vc-class)# end
```

Additional References

Related Documents

Related Topic	Document Title
ATM commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Asynchronous Transfer Mode Command Reference*
SNMP commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Overview of ATM SPAs	"Configuring ATM"

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-ATM-IF-MIB • CISCO-ATM-PVC-MIB • CISCO-ATM-PVCTRAP-EXTN-MIB • CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ATM SNMP Trap and OAM Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 8: Feature Information for Configuring ATM SNMP Trap and OAM Enhancements

Feature Name	Releases	Feature Information
ATM SNMP Trap and OAM Enhancements	Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.2S	The feature provides enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to Operation, Administration, and Maintenance (OAM) functionality. The ATM SNMP Trap and OAM Enhancements feature introduces a high watermark trap. A trap is generated when the number of configured PVCs in an interface and related subinterfaces exceeds a preconfigured high watermark threshold. The following commands were introduced or modified: **oam-pvc manage**, **rmon alarm, snmp-server enable traps atm pvc extension**.
ATM OAM AIS-RDI Monitoring	Cisco IOS XE Release 2.3	The ATM OAM AIS-RDI Monitoring feature extends the existing ATM virtual circuit OAM functionality to include monitoring of the AIS-RDI. The following commands were introduced or modified: **oam ais-rdi**.

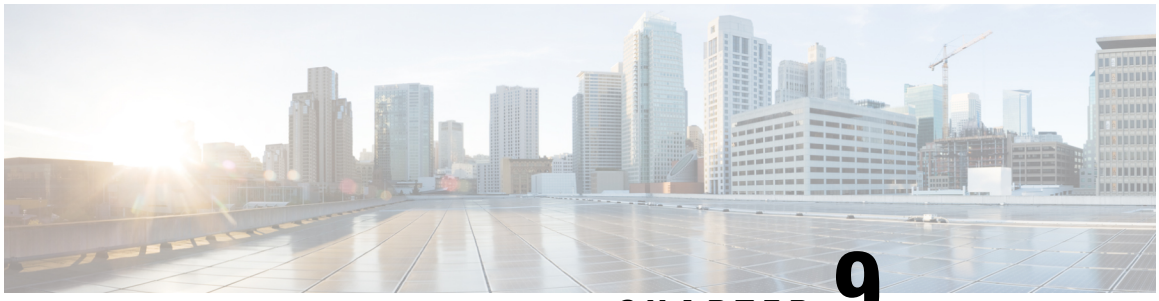
Glossary

LFI --link fragmentation and interleaving. Method of fragmenting large packets and then queueing the fragments between small packets.

MLP --multilink PPP.

QoS --quality of service.

VC --virtual circuit.



CHAPTER 9

ATM PVC F5 OAM Recovery Traps

The ATM PVC F5 OAM Recovery Traps feature introduces Simple Network Management Protocol (SNMP) traps that notify the administrator when a permanent virtual circuit (PVC) has recovered from F5 Operation, Administration, and Maintenance (OAM) end-to-end loopback failures, and F5 OAM alarm indication signal/remote defect indication (AIS/RDI) failures.

Prerequisites for ATM PVC F5 OAM Recovery Traps

Extended ATM PVC up and down traps and ATM PVC traps for, OAM F5 AIS/RDI, and OAM F5 loopback failures and recoveries cannot be used at the same time as the legacy ATM PVC trap. The legacy ATM PVC trap must be disabled by using the **no snmp-server enable traps atm pvc** command before extended ATM PVC up and down traps and ATM PVC traps for OAM F5 CC, OAM F5 AIS/RDI, and OAM F5 loopback failures and recoveries can be configured.

OAM management must be enabled on the PVC before you can use any ATM PVC traps.

Restrictions for ATM PVC F5 OAM Recovery Traps

The F5 OAM recovery traps are supported for ATM PVCs only.

Information About ATM PVC F5 OAM Recovery Traps

F5 OAM Recovery Traps for ATM PVCs

F5 OAM cells are used to detect connectivity failures and recoveries at the ATM layer. Before the introduction of this feature, Cisco IOS software provided support for SNMP traps (also called SNMP notifications) for F5 end-to-end loopback, and F5 AIS/RDI connectivity failures on a PVC. The ATM PVC F5 OAM Recovery Traps feature introduces SNMP traps that notify the network management system (NMS) when connectivity is restored to a PVC after the following types of failures:

- F5 OAM end-to-end loopback failures
- F5 OAM segment AIS/RDI failures
- F5 OAM end-to-end AIS/RDI failures

Information in the traps includes the number of PVCs that recovered and time stamps indicating when the first and last recoveries occurred during the notification interval.

To limit the amount of traffic that can be generated by the F5 OAM failure and recovery traps, only one trap of each type can be generated in each trap interval. Each trap can report on multiple PVCs, and successive PVCs that have the same failure or recovery are reported as a range.

In addition to the traps, MIB tables are maintained to provide information about the failures and recoveries on PVCs.

For a complete description of the extended ATM PVC Trap MIB, including the supported notifications and tables, see the MIB file called CISCO-ATM-PVCTRAP-EXTN-MIB.my, available through Cisco.com at the following URL:

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

Benefits of F5 OAM Recovery Traps for ATM PVCs

Before the introduction of this feature, when F5 OAM failures were detected on PVCs, failure notifications were sent to the NMS, and the operational state of the PVC was kept up. There was no mechanism for notifying the NMS when connectivity was restored to the PVCs after F5 OAM failures. The F5 OAM Recovery Traps feature introduces traps that asynchronously notify the NMS when PVCs have recovered from F5 OAM failures.

How to Configure F5 OAM Recovery Traps for ATM PVCs

Configuring ATM OAM Support

Perform this task to configure ATM OAM support on an ATM PVC.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface atm** *number*
4. **ip address** *ip-address mask*
5. **pvc** [*name*] *vpi* / *vci*
6. **oam-pvc manage** [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.0.0.3 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 0/40`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 6	**oam-pvc manage** [**keep-vc-up** [**end aisrdi failure** | **seg aisrdi failure**]] **Example:** `Router(config-if-atm-vc)# oam-pvc manage`	Configures ATM OAM management.

Enabling OAM F5 Failure and Recovery Traps

Perform this task to enable the MIB and SNMP notifications that support ATM OAM F5 CC management.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **snmp-server enable traps atm pvc extension** {**up** | **down** | **oam failure** [**aisrdi** | **loopback** }

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps atm pvc extension** {**up**	**down**	**oam failure** [**aisrdi**	**loopback** } **Example:** `Router(config)# snmp-server enable traps atm pvc extension oam failure aisrdi`	Enables ATM OAM F5 AIS/RDI failure and recovery traps and ATM OAM F5 end-to-end loopback failure and recovery traps.

Troubleshooting Tips

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp authentication**
- **debug ppp negotiation**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**
- **debug aaa authorization**

Caution Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

Configuration Examples for ATM PVC F5 OAM Recovery Traps

Enabling OAM PVC Managment Example

The following example shows how to enable ATM PVC OAM management.

```
Router(config)# interface ATM0/3/0.100 point-to-point

Router(config-subif)# pvc pvc100 0/100

Router(config-if-atm-vc)# oam-pvc manage
Router(config-if-atm-vc)# end
```

Note Enhanced Interior Gateway Routing Protocol (EIGRP) must be configured on the router if you want the notification packets to be sent to the NMS.

ATM PVC Extended Up and Down Notifications Example

Enabling ATM PVC extended up and down notifications: Example

The following example shows how to enable ATM PVC extended up and down notifications:

```
snmp-server community public RW
snmp-server host 172.16.61.90 public
snmp-server enable traps atm pvc extension up
snmp-server enable traps atm pvc extension down
snmp-server host 10.0.0.115 vrf Mgmt-intf version 2c public udp-port 2030
```

ATM PVC Down Notification: Example

The following sample output shows an ATM PVC in the DOWN state:

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
           VCD /                                              Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              DN
```

The following example shows the corresponding output for the ATM PVC extended down notification:

```
Received SNMPv2c Trap:
Community: public
From: 10.0.0.54
sysUpTimeInstance = 1918435
snmpTrapOID.0 = catmIntfPvcDownTrap
ifIndex.52 = 52
atmIntfPvcFailures.15 = 4
atmIntfCurrentlyFailingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclCurFailTime.52.0.100 = 1915435
catmPVclPrevRecoverTime.52.0.100 = 259552
catmPVclFailureReason.52.0.100 = catmLoopbackOAMFailure(1)
```

ATM PVC Up Notification: Example

The following sample output shows an ATM PVC in the UP state:

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
```

```
           VCD /                                                Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC      Kbps   Kbps Cells St
0/3/0.100  pvc100          0   100 PVC     SNAP       UBR  149760              UP
```

The following example shows the corresponding output for the ATM PVC extended up notification:

```
Received SNMPv2c Trap:
Community: public
From: 9.0.0.54
sysUpTimeInstance = 1933376
snmpTrapOID.0 = catmIntfPvcUp2Trap
ifIndex.52 = 52
catmIntfCurrentlyDownToUpPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclCurRecoverTime.52.0.100 = 1930676
catmPVclPrevFailTime.52.0.100 = 1915435
catmPVclRecoveryReason.52.0.100 = catmLoopbackOAMRecover(1)
```

ATM OAM Failure Looback Notification Example

Enabling ATM OAM Failure Loopback Notification: Example

```
The following example shows how to enable ATM PVC OAM failure loopback notifications and
extended up and down notifications:
snmp-server community public RW
snmp-server enable traps atm pvc extension up
snmp-server enable traps atm pvc extension down
snmp-server enable traps atm pvc extension oam failure loopback
snmp-server host 10.0.0.115 vrf Mgmt-intf version 2c public udp-port 2030
```

Note If you configure the **snmp-server enable traps atm pvc extension oam failure** command, you may not see up or down traps when an OAM failure trap is generated. Additionally, the PVC will stay in the UP state.

OAM Loopback Failure Notification: Example

The following sample output shows an ATM PVC that has failed. Note that the output indicates the PVC is still in the UP state.

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
           VCD /                                                Peak Av/Min Burst
Interface  Name          VPI   VCI Type    Encaps     SC      Kbps   Kbps Cells St
0/3/0.100  pvc100          0   100 PVC     SNAP       UBR  149760              UP
```

The following example shows the corresponding output for the OAM loopback failure notification:

```
Received SNMPv2c Trap:
Community: public
From: 9.0.0.54
sysUpTimeInstance = 1964155
snmpTrapOID.0 = catmIntfPvcOAMFailureTrap
ifIndex.52 = 52
catmIntfOAMFailedPVcls.15 = 65
catmIntfCurrentOAMFailingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
```

```
catmPVclStatusTransition.52.0.100 = 1
catmPVclStatusChangeStart.52.0.100 = 1961155
catmPVclStatusChangeEnd.52.0.100 = 1961155
```

OAM Loopback Recovery Notification: Example

The following sample output shows an ATM PVC in the UP state:

```
Router# show atm vc
Codes: DN - DOWN, IN - INACTIVE
           VCD /                                              Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
0/3/0.100  pvc100         0   100 PVC     SNAP       UBR  149760              UP
```

The following example shows the corresponding output for the OAM loopback recovery notification:

```
Received SNMPv2c Trap:
Community: public
From: 9.0.0.54
sysUpTimeInstance = 1986456
snmpTrapOID.0 = catmIntfPvcOAMRecoverTrap
ifIndex.52 = 52
catmIntfOAMRcovedPVcls.15 = 10
catmIntfCurrentOAMRcovingPVcls.15 = 1
ifDescr.52 = ATM0/3/0.100
catmPVclStatusUpTransition.52.0.100 = 1
catmPVclStatusUpStart.52.0.100 = 1983456
catmPVclStatusUpEnd.52.0.100 = 1983456
```

Additional References

Related Documents

Related Topic	Document Title
OAM and ATM PVC trap support commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature.	--

MIBs

MIBs	MIBs Link
• CISCO-ATM-PVCTRAP-EXTN-MIB.my.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this features.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

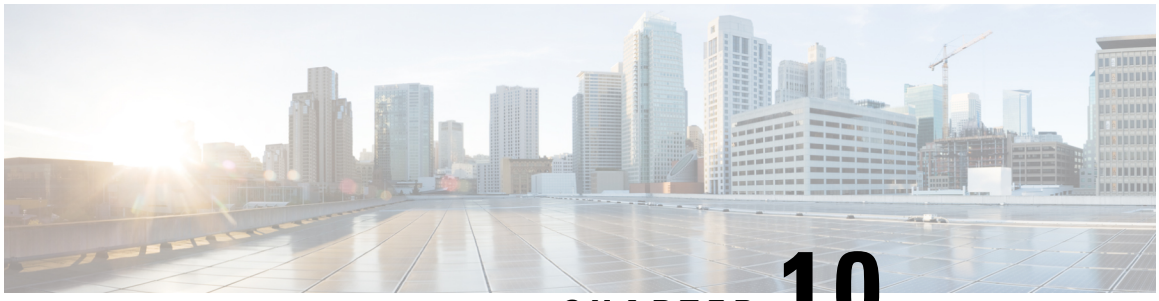
Feature Information for ATM PVC F5 OAM Recovery Traps

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 9: Feature Information for ATM PVC F5 OAM Recovery Traps

Feature Name	Releases	Feature Information
ATM PVC F5 OAM Recovery Traps	Cisco IOS XE Release 2.3	The ATM PVC F5 OAM Recovery Traps feature introduces SNMP traps that notify the administrator when a PVC has recovered from F5 OAM end-to-end loopback failures and F5 OAM AIS/RDI failures. The following command was introduced: **snmp-server enable traps atm pvc extension**.



CHAPTER 10

ATM VP Average Traffic Rate

The ATM VP Average Traffic Rate feature is a subscriber and VP traffic reporting feature that enables you to display the 5-minute traffic rates on virtual path (VP) counters.

Information About ATM VP Average Traffic Rate

ATM VP Average Traffic Rate

The ATM VP Average Traffic Rate feature is a subscriber and VP traffic reporting feature that enables you to display the 5-minute traffic rates on virtual path (VP) counters. This feature extends the **show atm vp** command to provide rate information. Minute counters on the ATM VPs support the **show atm vp** command.

The ATM VP Average Traffic Rate feature provides support for VP-based rate counters and enables you to display the average traffic load on the VP for the last 5 minutes. This feature is enabled by default and requires no configuration. The duration of the counters is set at 5 minutes average.

How to Display ATM VP Average Traffic Rates

Displaying ATM VP 5-Minute Traffic Rates

To display the 5-minute traffic rates, use the following command in privileged EXEC mode:

Command	Purpose
`Router# show atm vp [vpi]`	Displays statistical information, including the 5-minute traffic rate, for all virtual paths (VPs) on an interface or for a specific VP. • (Optional) *vpi* is the ATM network virtual path identifier (VPI) of the permanent virtual path. The range is from 0 to 255. The VPI is an 8-bit field in the header of the ATM cell.

Configuration Examples for ATM VP Average Traffic Rates

ATM VP 5-Minute Traffic Rates Example

The following example shows sample output from the **show atm vp** command. The output displays the 5-minute traffic rates for VP 10:

```
Router# show atm vp 10

ATM1/1/0 VPI: 10, PeakRate: 100000, CesRate: 0, DataVCs: 1, CesVCs: 0, Status: INACTIVE
VCD VCI  Type InPkts  OutPkts  AAL/Encap   Status
1   3    PVC      0        0    F4 OAM     INACTIVE
2   4    PVC      0        0    F4 OAM     INACTIVE
3  100   PVC   78310    78310  AAL5-SNAP    ACTIVE
TotalInPkts: 78310, TotalOutPkts: 78310, TotalInFast: 0, TotalOutFast: 0, TotalBroadcasts:

5 Min Average Output Rate: 0 packets/sec, 32 bits/sec
TotalInPktDrops: 0, TotalOutPktDrops: 0
Total subscribed rate of active VC's: 0
```

Additional References

Related Documents

Related Topic	Document Title
show atm vp command	*Cisco IOS Asynchronous Transfer Mode Command Reference*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

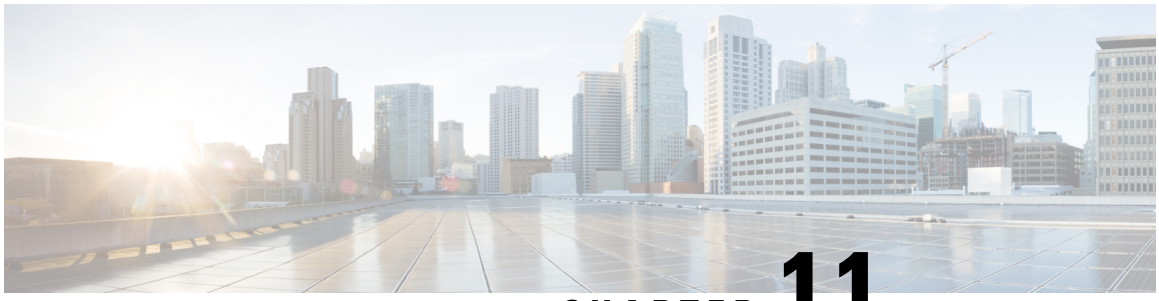
Feature Information for ATM VP Average Traffic Rate

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 10: Feature Information for ATM VP Average Traffic Rate

Feature Name	Releases	Feature Information
ATM VP Average Traffic Rate	Cisco IOS XE Release 2.3	Enables you to display 5-minute traffic rates at the VP level. The following command was modified: show atm vp.



CHAPTER 11

ATM Hierarchical Shaping ATM VC into VP Shaping

Traffic shaping is a quality of service (QoS) mechanism that is used to manage the network traffic by shaping the traffic to a specified rate. Traffic shaping enables the network administrator to:

- Control access to the available bandwidth.
- Ensure that the traffic conforms to the policies.
- Regulate the flow of traffic to avoid congestion that can occur when the transmitted traffic exceeds the access speed of its remote target interface.

Traffic shaping uses queues to constrain data bursts, limit peak data rate, and smooth jitters so that traffic will fit within the promised envelope. Traffic shaping limits the throughput by buffering excess traffic instead of dropping packets.

ATM VP/VC hierarchical shaping provides two levels of traffic shaping--per-VC and per-VP--to control or modify the flow of traffic on an interface. The shaping function also ensures that the traffic from one VC does not adversely impact another VC, thus preventing the loss of data. The traffic is shaped first at the VC level and then at the VP level.

Restrictions for ATM Hierarchical Shaping

All virtual channels (VCs) within a given virtual path (VP) must belong to the same ATM service category.

Information About ATM Hierarchical Shaping

ATM Hierarchical Shaping

If a service (or an application) wants to use an ATM network to transport a particular kind of traffic, it must first inform the network about what kind of traffic is to be transported, and the performance requirements of that traffic. The ATM service categories provide a method to relate traffic characteristics and QoS requirements to network behavior. Hierarchical shaping requires that all VCs belonging to a given VP have the same ATM service category. This hierarchy ensures that packets are shaped first at the VC level and then at the VP level. At the interface level, the priority is based on the ATM service category. The service category is determined by the first PVC that is configured under a VP. The priority is in the following order:

1. Constant Bit Rate (CBR)
2. Unspecified Bit Rate (UBR)
3. Unspecified Bit Rate + (UBR+)
4. Variable Bit Rate Non Real-Time (VBR-nRT)
5. Real-time Variable Bit Rate (VBR-RT)

If no service category is specified at the VC level, the default is unshaped UBR. The ATM Hierarchical Shaping feature is supported for the all the above ATM traffic service categories.

For VBR-nRT traffic the output sustainable cell rate (SCR) value that is configured will be taken into account for VC shaping. For UBR traffic, the output peak cell rate (PCR) value that is configured will be taken into account for VC shaping.

The ATM Hierarchical Shaping feature supports over-subscription. Over-subscription occurs when the sum of the configured rate of UBR and VBR PVCs exceeds the line rate.

How to Configure ATM Hierarchical Shaping

Configuring ATM Hierarchical Shaping

Perform this task to configure ATM hierarchical shaping.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** *vpi* **/** *vci*
5. **exit**
6. **ubr** *output-pcr*
7. **exit**
8. **create on-demand**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 0/3/2.1 point-to-point`	Configure an ATM interface and enters subinterface configuration mode.
Step 4	**pvc** *vpi* **/** *vci* **Example:** `Router(config-subif)# pvc 2/200`	Creates or assigns a name to an ATM PVC and enters ATM virtual circuit configuration mode.
Step 5	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to subinterface configuration mode.
Step 6	**ubr** *output-pcr* **Example:** `Router(config-if-atm-vc)# ubr`	Configures UBR QoS and specifies the output PCR for an ATM PVC, PVC range, switched virtual circuit (SVC), VC class, or VC bundle member.
Step 7	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to subinterface configuration mode.
Step 8	**create on-demand** **Example:** `Router(config-if-atm-vc)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a PVC or range of PVCs to be created automatically on demand.

Configuration Examples for ATM Hierarchical Shaping

Example Configuring ATM Hierarchical Shaping

The following example shows how to configure ATM hierarchical shaping:

```
enable
 configure terminal
  interface atm 0/3/2.1 multipoint
   atm pvp 2
   pvc 2/200
    exit
   range range1 pvc 2/100 2/102
    ubr 4000
    exit
   atm pvp 3
   pvc 3/100
    vbr-nrt 1000 1000
    create on-demand
    end
```

Additional References

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

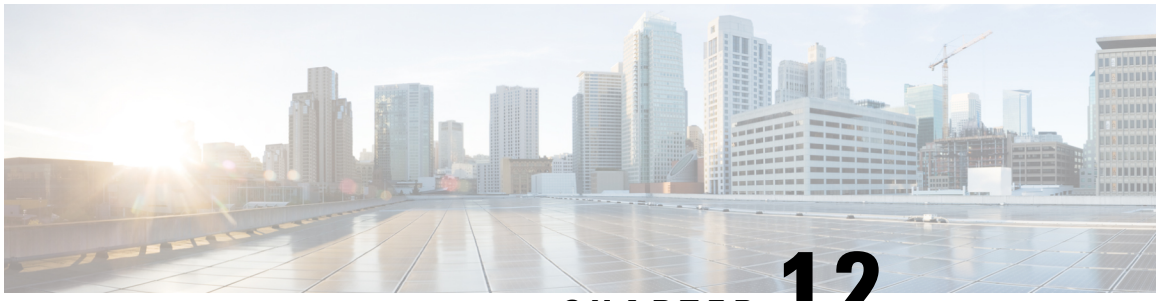
Feature Information for ATM Hierarchical Shaping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 11: Feature Information for ATM Hierarchical Shaping

Feature Name	Releases	Feature Information
ATM Hierarchical Shaping--ATM VC into VP Shaping	Cisco IOS XE Release 3.3S	ATM VP/VC hierarchical shaping provides two levels of traffic shaping--per-VC and per-VP--to control or modify the flow of traffic on an interface. The shaping function also ensures that traffic from one VC does not adversely impact another VC, thus preventing loss of data. The traffic is shaped first at the VC level and then at the VP level.



CHAPTER 12

Autosense for ATM PVCs and MUX SNAP Encapsulation

The PPPoA/PPPoE Autosense for ATM PVCs feature enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPPoA/PPPoE autosense functionality by providing autosense support on multiplexer (MUX) and Subnetwork Access Protocol (SNAP)-encapsulated ATM permanent virtual circuits (PVCs).

Restrictions for Autosense

- Do not use this feature on a router that initiates PPPoA sessions.
- PPPoA does not support static IP assignments within virtual templates.
- The PPPoE autosense is supported only for SNAP-encapsulated sessions.
- This feature supports ATM PVCs. Switched virtual circuits (SVCs) are not supported.

Information About Autosense

PPPoA PPPoE Autosense

PPPoA/PPPoE autosense enables a router to distinguish between incoming PPPoA and PPPoE over ATM sessions and to create virtual access based on demand for both PPP types.

Autosense of MUX SNAP Encapsulation on ATM PVCs

The Autosense of MUX/SNAP Encapsulation on ATM PVCs feature enables the PVC encapsulation type to be autosensed by the router. The router determines the encapsulation type of a PVC by looking at the encapsulation type of the first incoming packet. If the PVC encapsulation type is changed while the PPPoA or PPPoE session on the network access server (NAS) is still up, the incoming packet is dropped, the encapsulation type is reset to autosense, and all sessions are removed from the PVC. The next incoming packet will then determine the new encapsulation type of the PVC.

Benefits of Autosense of PPPoA PPPoE for MUX SNAP Encapsulation

The Autosense of PPPoA/PPPoE for MUX or SNAP Encapsulation feature provides resource allocation on demand. For each PVC configured for both PPPoA and PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoA or PPPoE session on that PVC. With the Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature, resources are allocated for PPPoA and PPPoE sessions only when a client initiates a session, thus reducing overhead on the network access server (NAS).

This feature also saves configuration time by eliminating the need to specify the encapsulation type when ATM PVCs are being provisioned and by eliminating the need to manually provision ATM PVCs each time the encapsulation type changes.

How to Configure PPPoA PPPoE Autosense on ATM PVCs

Configuring PPPoA PPPoE Autosense on a PVC

Perform this task to configure PPPoA/PPPoE Autosense on a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci*
5. **encapsulation aal5autoppp virtual-template** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**interface atm** *number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 2/2/0.2 multipoint`	Specifies the ATM interface and optional subinterface and enters subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc pvc1 45/54`	Configures a PVC on the ATM interface or subinterface and enters ATM VC configuration mode.
Step 5	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-if-atm-vc)# encapsulation aal5autoppp virtual-template 3`	Configures PPPoA/PPPoE autosense on the PVC. • Also specifies the virtual template interface to use to clone the new virtual-access interfaces for PPP sessions on this PVC.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Ends the session and enters privileged EXEC mode.

Configuring PPPoA PPPoE Autosense on a VC Class

Note Virtual-access interfaces for PPPoE sessions are cloned from the virtual template interface specified in the virtual private dialup network (VPDN) group.

Perform this task to configure PPPoA/PPPoE autosense on a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation aal5autoppp virtual-template** *number*
5. **exit**
6. **interface atm** *number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}]
7. **class-int** *vc-class-name*
8. **end**
9. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm vc1`	Creates and names a map class and enters VC class configuration mode.
Step 4	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-vc-class)# encapsulation aal5autoppp virtual-template 4`	Configures PPPoA/PPPoE autosense. • Also specifies the virtual template interface to use to clone the new virtual-access interfaces for PPP sessions on this PVC.
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Returns to global configuration mode.
Step 6	**interface atm** *number* [**.** *subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 2/2/0.2 multipoint`	Specifies the ATM interface and enters subinterface configuration mode.
Step 7	**class-int** *vc-class-name* **Example:** `Router(config-subif)# class-int vc1`	Applies the VC class to all VCs on the ATM interface or subinterface.
Step 8	**end** **Example:** `Router(config-subif)# end`	Ends the session and enters privileged EXEC mode.
Step 9	**show running-config** **Example:** `Router#  show running-config`	Verifies whether the PPPoA/PPPoE autosense configuration is successful.

Troubleshooting Tips

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp authentication**
- **debug ppp negotiation**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**
- **debug aaa authorization**

Caution Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

Monitoring and Maintaining PPPoA PPPoE Autosense for ATM PVCs

Perform this task to monitor and maintain PPPoA/PPPoE autosense for ATM PVCs. The **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show atm pvc** [**ppp**]
3. **show caller**
4. **show interface virtual-access** *interface-number*
5. **show user**
6. **show vpdn**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm pvc** [**ppp**] **Example:** `Router# show atm pvc ppp`	Checks that the PVC contains the PPPoA session after the client at the other end of the PVC has initiated a PPPoA session.
Step 3	**show caller** **Example:**	Displays caller information. • Use this command to:

	Command or Action	Purpose
	`Router# show caller`	• Display individual users and consumed resources on the NAS. • Inspect active call statistics for large pools of connections. (The **debug** commands produce too much output and tax the CPU too heavily.) • Display the absolute and idle times for each user. The current values for both of these settings are displayed on the tty line and the asynchronous interface. Users that have been idle for unacceptably long periods of time can be easily identified. You can use this information to define timeout policies and multiple grades of services for different users.
Step 4	**show interface virtual-access** *interface-number* **Example:** `Router# show interface virtual-access 1`	Displays information about the virtual-access interface, link control protocol, protocol states, and interface statistics. • The status of the virtual-access interface should read: Virtual-Access3 is up, line protocol is up
Step 5	**show user** **Example:** `Router# show user`	Displays information about the active lines on the router.
Step 6	**show vpdn** **Example:** `Router# show vpdn`	Displays basic information about all active VPDN tunnels.

Configuration Examples for Autosense for ATM PVCs

Example PPPoA PPPoE Autosense on an ATM PVC

The following example shows how to configure the NAS with PPPoA/PPPoE autosense on PVC 30/33:

```
! Configure PPP Autosense
!
interface atm 0/0/0.33 multipoint
 pvc 30/33
  encapsulation aal5autoppp virtual-template 1
  protocol pppoe
!
interface virtual-template 1
 ip unnumbered fastethernet 0/0/0
 ip route-cache cef
!
interface fastethernet 0/0/0
```

```
 ip address 10.1.1.1 255.255.255.0
!
```

Example PPPoA PPPoE Autosense on a VC Class

The following example shows how to configure the NAS with PPPoA/PPPoE autosense on the VC class called MyClass. The MyClass VC class applies PPPoA/PPPoE autosense to all PVCs on the ATM 0/0/0.99 interface.

```
! Configure PPP Autosense
!
vc-class atm MyClass
 encapsulation aal5autoppp virtual-template 1
!
interface atm 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
  protocol pppoe
!
interface virtual-template 1
  ip unnumbered fastethernet 0/0/0
  ip route-cache cef
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
```

Example PPPoA PPPoE Autosense on Multiple VC Classes and Virtual Templates

The following example shows how to handle PPPoA and PPPoE sessions separately using two virtual templates:

```
interface atm 0/0/0.3 multipoint
 no ip directed-broadcast
 class-int pppauto
!
interface atm 0/0/0.9 multipoint
 ip address 10.16.40.1 255.255.0.0
 no ip directed-broadcast
!
interface virtual-template 1
 ip unnumbered atm 0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-1
 ppp authentication pap
!
interface virtual-template 2
 ip unnumbered atm 0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-2
 ppp authentication chap
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
```

```
!
vc-class atm pppauto
 encapsulation aal5autoppp virtual-template 2
!
```

Note Whenever possible, configure PPPoA and PPPoE to use the same virtual template. Using separate virtual templates leads to the inefficient use of virtual access because the maximum number of virtual-access interfaces will have to be precloned twice: once for PPPoE and once for PPPoA. If PPPoA and PPPoE use the same virtual template, the maximum number of virtual-access interfaces can be precloned once and used for PPPoA and PPPoE as needed.

Feature Information for Autosense for ATM PVCs and MUX SNAP Encapsulation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 12: Feature Information for Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs

Feature Name	Releases	Feature Information
PPPoA/PPPoE Autosense for ATM PVCs	Cisco IOS XE Release 3.3S	The PPPoA/PPPoE Autosense for ATM PVCs feature enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.
Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs	Cisco IOS XE Release 3.3S	The Autosense of MUX/SNAP Encapsulation and PPPoA/PPPoE on ATM PVCs feature enhances PPP over ATM (PPPoA)/PPP over Ethernet (PPPoE) autosense functionality by providing autosense support on MUX- and SNAP-encapsulated ATM permanent virtual circuits (PVCs). The following command was introduced or modified: **encapsulation aal5autoppp virtual-template**.

Glossary

cloning --Creating and configuring a virtual-access interface by applying a specific virtual template interface. The template is the source of the generic user information and router-dependent information. The result of cloning is a virtual-access interface configured with all the commands in the template.

LCP --Link Control Protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

NAS --network access server. A device providing local network access to users across a remote access network such as the public switched telephone network (PSTN).

PPP --Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

PPPoA --PPP over ATM.

PPPoE --PPP over Ethernet.

precloning --Cloning a specified number of virtual-access interfaces from a virtual template at system startup or when the command is configured.

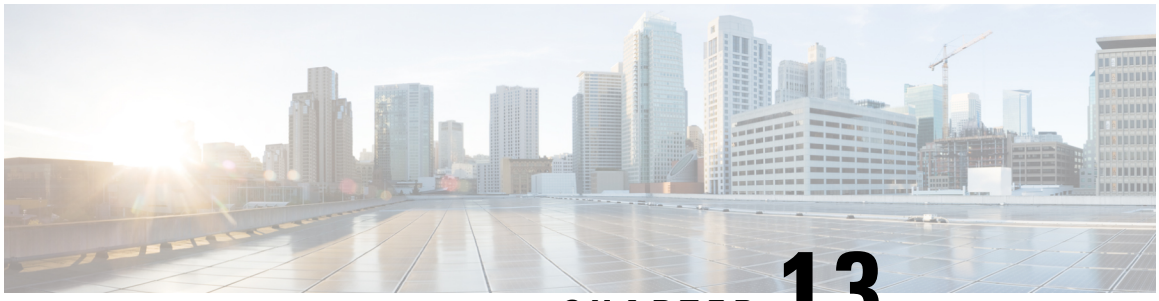
PVC --permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

VC --virtual channel. Logical circuit created to ensure reliable communication between two network devices. A VC is defined by a VPI/VCI pair and can be either permanent (PVC) or switched (SVC).

virtual-access interface --Instance of a unique virtual interface that is created dynamically and exists temporarily. Virtual-access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks. Virtual-access interfaces are cloned from virtual template interfaces.

virtual template interface --A logical interface configured with generic configuration information for a specific purpose or configuration common to specific users, plus router-dependent information. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual-access interfaces, as needed.

VPDN --virtual private dialup network. A system that permits dial-in networks to exist remotely from home networks, while giving the appearance of being directly connected.



CHAPTER 13

N:1 PVC Mapping to PWE with Nonunique VPIs

The N:1 PVC Mapping to PseudoWire Emulation (PWE) with Nonunique virtual path identifiers (VPIs) feature maps one or more ATM permanent virtual circuits (PVCs) to a single pseudowire (PW). There are two modes of AAL0 encapsulation, N:1 and 1:1 mapping. In N:1 mapping, multiple unrelated virtual path identifier/virtual channel identifier (VPI/VCI) are carried over a single Multiprotocol Label Switching (MPLS) PW. This is an efficient mapping method because less resources are used from the MPLS network. In 1:1 mapping, a single VPI/VCI is carried over a single MPLS PW. Benefits of this feature include the following:

- Aggregate quality of service (QoS) can be applied to related PVCs.
- Bandwidth is conserved with the reduction in the number of pseudowires that are used.

Restrictions for N:1 PVC Mapping to PWE with Nonunique VPIs

- N:1 permanent virtual circuits (PVC) mapping configuration is supported only on multipoint subinterfaces; it is not supported on main interfaces or point-to-point subinterfaces.
- N:1 PVC mapping mode is not supported on Access Circuit Redundancy subinterfaces.
- Preconfigured PVCs cannot exist on the multipoint subinterface on which you want to configure N:1 PVC mapping.
- An attachment circuit that has been bound to a pseudowire cannot be removed unless all Layer 2 virtual circuits (VCs) have been removed.
- Layer 3 PVCs cannot be configured on N:1 subinterfaces.
- Cell packing values configured under a VC class attached to the PVC, main interface, or subinterface will not be inherited by N:1 PVCs.
- Operation, Administration, and Maintenance (OAM) functionality is not supported on N:1 Layer 2 PVCs. OAM cells coming from the customer edge (CE) network will be treated as normal data traffic and will traverse through the pseudowire.

- Only ATM adaptation layer type 0 (AAL0) encapsulation is supported for N:1 PVCs.
- The service policy configuration can be configured only at the subinterface level for N:1 PVCs.

Information About N:1 PVC Mapping to PWE with Nonunique VPIs

N:1 PVC Mapping to PWE with Nonunique VPIs Feature Description

To transport ATM cells over Multiprotocol Label Switching (MPLS), a VC is established between the provider edge (PE) routers on both ends of the MPLS backbone. With the N:1 permanent virtual circuit (PVC) Mapping to PseudoWire Emulation (PWE) with Nonunique VPIs feature, multiple PVCs irrespective of their Virtual Path Identifiers (VPIs), are transported over a single pseudowire configured on a subinterface. ("N:1" refers to the number of PVCs transported over one pseudowire). ATM cells are packed together in a single frame and sent over the single pseudowire. The ATM cell header information is packed together with the cell payload on a per-cell basis in the packets so that packets received at the egress end are unpacked and the ATM cells are mapped to the respective PVCs.

In N:1 PVC mapping mode, the device can pack cells only from a single PVC in an MPLS packet to transmit over a pseudowire; cells from multiple PVCs cannot be packed in a single MPLS packet and mapped to a single pseudowire for transmission. However, if a device receives an MPLS packet that is packed with cells from multiple PVCs, then those cells will be unpacked and sent to the respective PVCs.

How to Configure N:1 PVC Mapping to PWE with Nonunique VPIs

Configuring N:1 PVC Mapping to PWE with Nonunique VPIs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/subslot/port*
4. **atm mcpt-timers** *timer1 timer2 timer3*
5. **exit**
6. **configure terminal**
7. **interface atm** *slot/subslot/port.subslot* **multipoint**
8. **no ip address**
9. **atm enable-ilmi-trap**
10. **cell-packing** *maxcells* **mcpt-timer** *timer-number*
11. **xconnect** *peer-ipaddress vc-id* **encapsulation mpls**
12. **pvc** *vpi/vci* **l2transport**

13. Repeat Step 12 for the number of PVCs that you want to configure.
14. **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 atm** *slot/subslot/port* **Example:** `Device(config)# interface atm 9/1/1`	Enables the ATM interface and enters interface configuration mode.
Step 4	**atm mcpt-timers** *timer1 timer2 timer3* **Example:** `Device(config-if)# atm mcpt-timers 100 200 300`	Sets the Maximum Cell Packing Timeout (MCPT) values in microseconds. • The MCPT timer sets the time for which the device waits for the raw cells (AAL0 encapsulation) to be packed into a single packet for punting to the pseudowire.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**interface atm** *slot/subslot/port.subslot* **multipoint** **Example:** `Device(config)# interface atm 9/1/1.1 multipoint`	Enters subinterface configuration mode and creates a multipoint subinterface on the given port on the specified ATM Shared Port Adapter (SPA).
Step 8	**no ip address** **Example:** `Device(config-subif)# no ip address`	Removes the interface IP address.
Step 9	**atm enable-ilmi-trap** **Example:** `Device(config-subif)# atm enable-ilmi-trap`	Generates an Integrated Local Management Interface (ILMI) atmfVccChange trap when an ATM interface or subinterface is enabled or shut down.

	Command or Action	Purpose
Step 10	**cell-packing** *maxcells* **mcpt-timer** *timer-number* **Example:** `Device(config-subif)# cell-packing 20 mcpt-timer 2`	Enables ATM over MPLS to pack multiple ATM cells into each MPLS packet within the MCPT timing.
Step 11	**xconnect** *peer-ipaddress vc-id* **encapsulation mpls** **Example:** `Device(config-subif)# xconnect 10.1.1.1 100 encapsulation mpls`	(Optional) Enables the attachment circuit and specifies the IP address of the peer, a VC ID, and the data encapsulation method.
Step 12	**pvc** *vpi/vci* **l2transport** **Example:** `Device(config-subif)# pvc 10/100 l2transport`	Assigns a VPI and virtual channel identifier (VCI).
Step 13	Repeat Step 12 for the number of PVCs that you want to configure.	—
Step 14	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuring N:1 PVC Mapping to PWE with Nonunique VPIs using the commands associated with the L2VPN Protocol-Based CLIs feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/subslot/port*
4. **atm mcpt-timers** *timer1 timer2 timer3*
5. **exit**
6. **configure terminal**
7. **interface atm** *slot/subslot/portt.subslot* **multipoint**
8. **no ip address**
9. **atm enable-ilmi-trap**
10. **cell-packing** *maxcells* **mcpt-timer** *timer-number*
11. **end**
12. **interface pseudowire** *number*
13. **encapsulation mpls**
14. **neighbor** *peer-address vcid-value*
15. **exit**
16. **l2vpn xconnect context** *context-name*
17. **member pseudowire** *interface-number*

18. **member gigabitethernet** *interface-number*
19. **end**
20. **pvc** *vpi*/*vci* **l2transport**
21. Repeat Step 12 for the number of PVCs that you want to configure.
22. **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 atm** *slot*/*subslot*/*port* **Example:** `Device(config)# interface atm 9/1/1`	Enables the ATM interface and enters interface configuration mode.
Step 4	**atm mcpt-timers** *timer1 timer2 timer3* **Example:** `Device(config-if)# atm mcpt-timers 100 200 300`	Sets the Maximum Cell Packing Timeout (MCPT) values in microseconds. • The MCPT timer sets the time for which the device waits for the raw cells (AAL0 encapsulation) to be packed into a single packet for punting to the pseudowire.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 7	**interface atm** *slot*/*subslot*/*portt.subslot* **multipoint** **Example:** `Device(config)# interface atm 9/1/1.1 multipoint`	Enters subinterface configuration mode and creates a multipoint subinterface on the given port on the specified ATM Shared Port Adapter (SPA).
Step 8	**no ip address** **Example:** `Device(config-subif)# no ip address`	Removes the interface IP address.

	Command or Action	Purpose
Step 9	**atm enable-ilmi-trap** **Example:** `Device(config-subif)# atm enable-ilmi-trap`	Generates an Integrated Local Management Interface (ILMI) atmfVccChange trap when an ATM interface or subinterface is enabled or shut down.
Step 10	**cell-packing** *maxcells* **mcpt-timer** *timer-number* **Example:** `Device(config-subif)# cell-packing 20 mcpt-timer 2`	Enables ATM over MPLS to pack multiple ATM cells into each MPLS packet within the MCPT timing.
Step 11	**end** **Example:** `Router(config-subif)# end`	Exits to privileged EXEC mode.
Step 12	**interface pseudowire** *number* **Example:** `Router(config)# interface pseudowire 100`	Specifies the pseudowire interface and enters interface configuration mode.
Step 13	**encapsulation mpls** **Example:** `Router(config-if)# encapsulation mpls`	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
Step 14	**neighbor** *peer-address vcid-value* **Example:** `Router(config-if)# neighbor 10.1.1.1 100`	Specifies the peer IP address and virtual circuit (VC) ID value of the Layer 2 VPN (L2VPN) pseudowire.
Step 15	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 16	**l2vpn xconnect context** *context-name* **Example:** `Router(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.
Step 17	**member pseudowire** *interface-number* **Example:** `Router(config-xconnect)# member pseudowire 100`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 18	**member gigabitethernet** *interface-number* **Example:**	Specifies the location of the Gigabit Ethernet member interface.

	Command or Action	Purpose
	`Router(config-xconnect)# member GigabitEthernet0/0/0.1`	
Step 19	**end** **Example:** `Router(config-xconnect)# end`	Exits to privileged EXEC mode.
Step 20	**pvc** *vpi*/*vci* **l2transport** **Example:** `Device(config-subif)# pvc 10/100 l2transport`	Assigns a VPI and virtual channel identifier (VCI).
Step 21	Repeat Step 12 for the number of PVCs that you want to configure.	—
Step 22	**end** **Example:** `Device(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuration Examples for N:1 PVC Mapping to PWE with Nonunique VPIs

Example: Configuring N:1 PVC Mapping to PWE with Nonunique VPIs

The following example shows how to configure the N:1 ATM permanent virtual circuit (PVC) mapping to pseudowires with non unique virtual path identifiers (VPIs):

```
Device> enable
Device# configure terminal
Device(config)# interface atm 9/1/1
Device(config-if)# atm mcpt-timers 500 5000 50000
Device(config-if)# exit
Device# configure terminal
Device(config)# interface atm 9/1/1.1 multipoint
Device(config-subif)# no ip address
Device(config-subif)# atm enable-ilmi-trap
Device(config-subif)# cell packing 20 mcpt-timer 2
Device(config-subif)# xconnect 10.1.1.1 100 encapsulation mpls
Device(config-subif)# pvc 10/100 l2transport
Device(config-subif)# pvc 11/122 l2transport
Device(config-subif)# pvc 19/231 l2transport
Device(config-subif)# end
```

Example: Configuring N:1 PVC Mapping to PWE with Nonunique VPIs using the commands associated with the L2VPN Protocol-Based CLIs feature

The following example shows how to configure the N:1 ATM permanent virtual circuit (PVC) mapping to pseudowires with non unique virtual path identifiers (VPIs):

```
Device> enable
Device# configure terminal
Device(config)# interface atm 9/1/1
Device(config-if)# atm mcpt-timers 500 5000 50000
Device(config-if)# exit
Device(config)# configure terminal
Device(config)# interface atm 9/1/1.1 multipoint
Device(config-subif)# no ip address
Device(config-subif)# atm enable-ilmi-trap
Device(config-subif)# cell packing 20 mcpt-timer 2
Device(config-subif)# exit
Device(config)#interface pseudowire 100
Device(config-if)#encapsulation mpls
Device(config-if)#neighbor 10.1.1.1 100
Device(config-if)# pvc 10/100 l2transport
Device(config-if)# pvc 11/122 l2transport
Device(config-if)# pvc 19/231 l2transport
Device(config-if)# exit
Device(config)#l2vpn xconnect context A
Router(config-xconnect)#member pseudowire 100
Device(config-xconnect)#member atm 9/1/1
Device(config-xconnect)# end
```

Additional References

Related Documents

Related Topic	Document Title
ATM commands	Asynchronous Transfer Mode Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

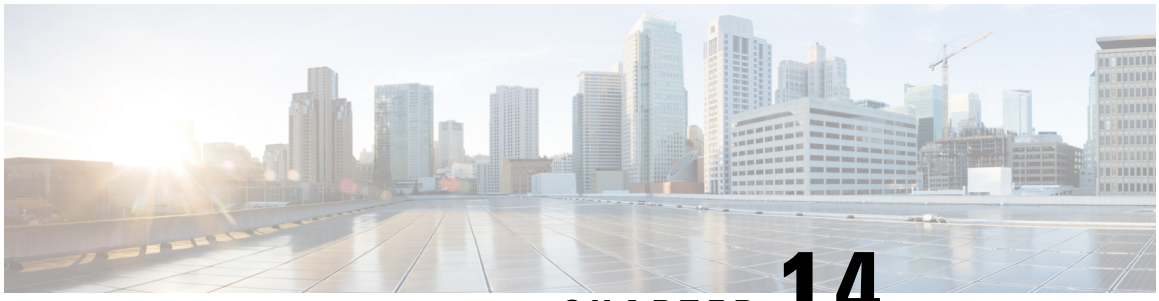
Feature Information for N:1 PVC Mapping to PWE with Nonunique VPIs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 13: Feature Information for N:1 PVC Mapping to PWE with Nonunique VPIs

Feature Name	Releases	Feature Information
N:1 PVC Mapping to PWE with Nonunique VPIs	Cisco IOS XE Release 3.7S	The N:1 PVC Mapping to PWE with Nonunique VPIs feature maps one or more ATM PVCs to a single pseudowire. In Cisco IOS XE Release 3.7S, support was added for Cisco ASR 903 Routers. The following command was introduced by this feature: **show atm cell-packaging** .



CHAPTER 14

Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1Q tags to be transported over ATM permanent virtual circuits (PVC) used in Asymmetric Digital Subscriber Line 2+ (ADSL2+) uplinks. Additionally, 802.1P marking is allowed and is based on 802.1Q tagging.

Note Although this document uses the generic term ADSL, this feature requires an ADSL2+ uplink.

Prerequisites for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

- You must have a basic understanding of ATM, bridging, DHCP, and VLANs before configuring this feature.

Restrictions for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

- Supports only one bridged 802.1Q VLAN.
- Can be configured only on a point-to-point ATM subinterface.
- Uses ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol (AAL5SNAP) encapsulation to enable the transport of an 802.1Q tag over an ATM PVC.

Information About Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Benefits of Preserve 802.1Q Tagging with 802.1P Marking

- CPE can carry traffic with 802.1P-marked provider-specific 802.1Q tags.
- Voice, video, and data services can be deployed at customer premises. This service combination offers a real-time channel dedicated to VoIP traffic and a second channel that delivers best-effort Internet service.
- All traffic is marked with an 802.1P marking which is implemented using VLAN-based service differentiation.

Note Support for PVCs configured with Route-Bridge Encapsulation (RBE) was introduced with CSCtt22809.

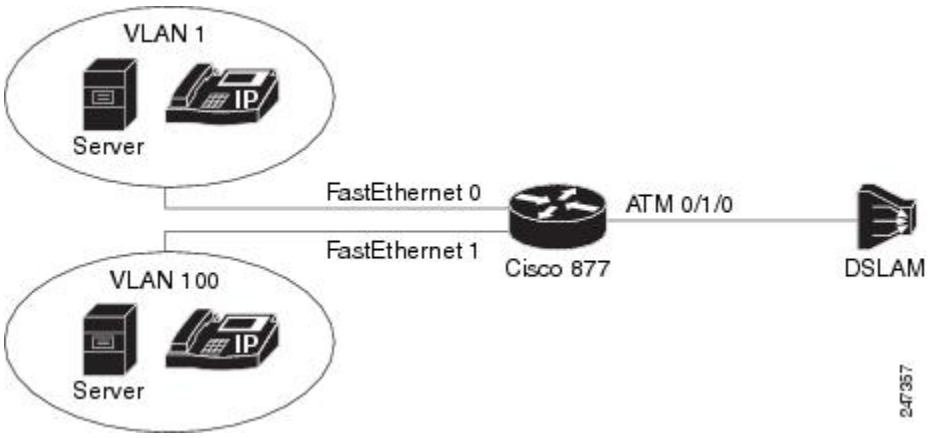
VLAN-Based Service Differentiation over ADSL

VLAN-based service differentiation allows service providers to offer a range of broadband-enabled services and applications to end users. It supports IP connectivity applications that require real-time network performance and applications that use best-effort, or Internet-grade performance.

The original VLAN tag in an inbound packet is changed to the value configured by the **bridge-dot1q encap** command before the tag leaves the device. For example, if you enter the command **bridge-dot1q encap 10**, a VLAN tag of 70 in a packet inbound from the local network is changed to a value of 10 in the egress packet. Any 802.1P value is changed to 0, and frames without VLAN tags are sent out over ATM with an added VLAN header as shown in the figure in the “Transporting 802.1P Marked 802.1Q Tags” section.

From an Ethernet perspective, this service is carried over a dedicated VLAN from the hand-over point to the end-user premises. This VLAN-based service differentiation at the PVC level is shown in the figure below.

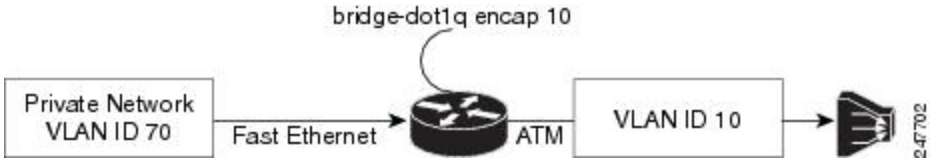
Figure 5: VLAN-Based Service Differentiation at PVC Level



The Ethernet VLAN used by the voice, video, and data services must be identified at the customer premises by an 802.1Q VLAN ID configured using the **bridge-dot1q encap** command. The VLAN is identified at the service provider's end by a service-provider-assigned 802.1ad customer VLAN ID.

The **bridge-dot1q encap** command changes the local VLAN ID to the VLAN ID required by the service provider. The operation of this command is shown in the figure below.

Figure 6: Operation of the bridge-dot1q encap Command



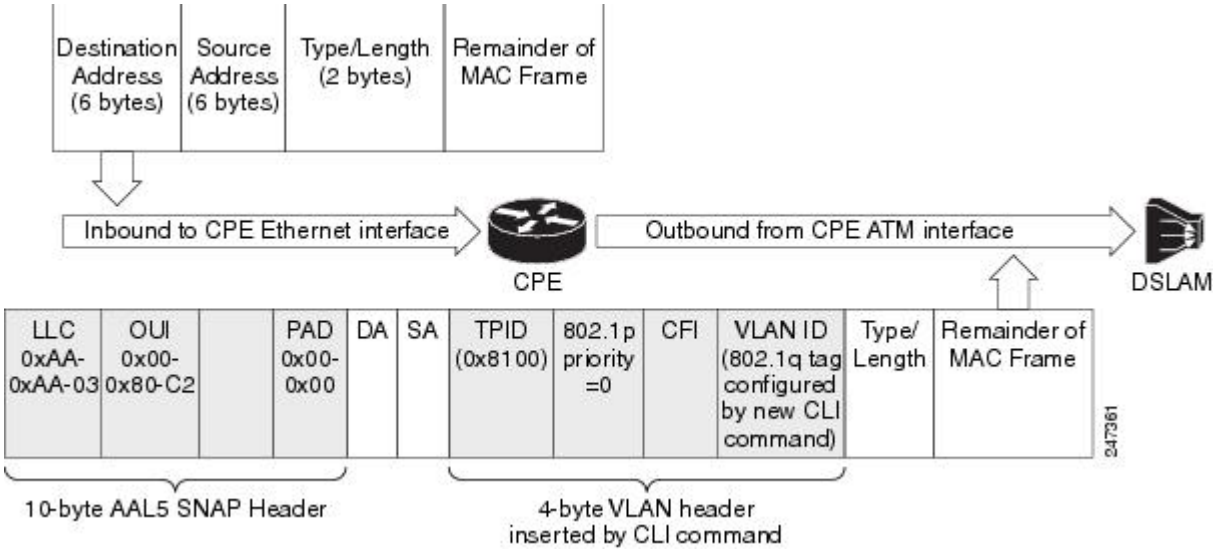
The figures in the "Transporting 802.1P Marked 802.1Q Tags" section show the PDU data structure in greater detail.

Transporting 802.1P Marked 802.1Q Tags

An 802.1Q VLAN tag is inserted into the MAC Protocol Data Unit (PDU), and this PDU is sent to the Digital Subscriber Line Access Multiplexer (DSLAM). Incoming and outgoing PDU structures are shown in the two figures below.

The figure below shows the packet structure when the incoming Ethernet frames do not have a VLAN header.

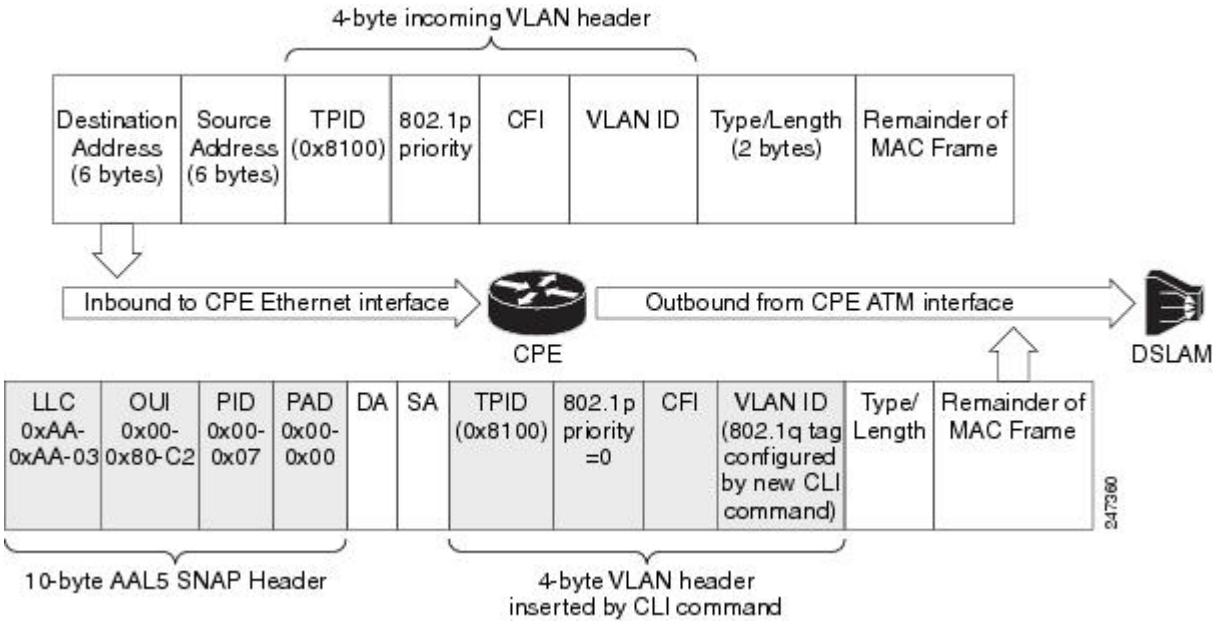
Figure 7: Incoming and Outgoing Packet Structures When No Incoming VLAN ID Is Present



The figure below shows that a 4-byte VLAN header has been inserted in the outgoing packet, with an 802.1P value. The VLAN ID value is configured by the **bridge-dot1q encap** command.

The figure below shows the incoming packet structure when the incoming Ethernet packets contain a VLAN header.

Figure 8: Incoming and Outgoing Packet Structures When an Incoming VLAN ID Is Present



The outgoing packet structure is the same as in figure 1.

Note The 802.1P priority that was configured earlier is changed to 0, and any VLAN ID that is configured is set to the ID configured by the **bridge-dot1q encap** command.

The CPE is connected to the DSLAM via an ATM interface that is configured as the bridging interface. The CPE establishes a PPP over Ethernet (PPPoE) session over the bridging ATM interface with the service provider. The VLAN and voice traffic enter customer devices via VLAN ports or a Switched Virtual Interface (SVI).

In the CPE, the packet is classified as data or voice traffic based on the VLAN ID, Differentiated Services Code Point (DSCP), protocol, source MAC address, or port. The packets are marked with the quality of service (QoS) group, and routed from VLAN via the Bridge Virtual Interface (BVI) to the ATM PVC bridging interface.

If the packet requires encapsulation, ATM provides the default VLAN ID. If there is a QoS service policy attached to the PVC, packets are classified against the QoS group. QoS marks the corresponding VLAN ID and 802.1P or class of service (CoS) value into the packet VLAN header. The QoS VLAN ID overwrites the default VLAN ID. If there is no service policy attached in PVC, the packets are sent out with the default VLAN ID and default CoS marking.

Packets returning from the service provider's network and destined to the customer's network carry VLAN tags. The ATM PVC interface removes the VLAN tag before passing it for further processing. These packets do not require classification or QoS marking.

Using PPPoE, the CPE device acts as a PPPoE Dialer client and gets the IP address dynamically from the service provider by using the Point-to-Point Protocol. The Dialer interface has to be configured and associated with the ATM PVC interface. The packets are sent out with the default VLAN ID as PPPoE supports only one VLAN ID per PVC. PPP control packets such as PPPoE Active Discovery Initiation (PADI), PPPoE Active Discovery Request (PADR), PPPoE Active Discovery Terminate (PADT) and keepalive packets are marked with higher priority CoS markings similar to the real-time traffic. The VLAN header has to be removed from the packet at the ingress interface (ATM PVC) when the packet returns.

How to Configure Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Configuring Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs

Perform this task to configure the Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature.

Note Only one **bridge-dot1q encap** *vlan-id* command can be configured under a PVC. Only one VLAN ID is allowed per session using PPPoE. The PPPoE session can be disconnected if the configured VLAN ID (set using the **set vlan-inner** or **bridge-dot1q encap** *vlanid* command) differs from the default VLAN ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-all egress**
4. **match qos-group** *number*
5. **class-map match-all ingress**
6. **match input-interface** *name*
7. **policy-map egress-policy**
8. **class egress**
9. **set cos** *number*
10. **set vlan-inner** *number*
11. **exit**
12. **exit**
13. **policy-map ingress-policy**
14. **class ingress**
15. **set qos-group** *number*
16. **exit**
17. **exit**
18. Enter one of the following:
    - **interface atm** *interface-id* **point-to-point**
    - **interface atm** *slot* **/ 0 point-to-point**
    - **interface atm** *slot/ port-adaptor*/**0 point-to-point**
19. **bridge-group** *group-number*
20. **pvc** *vpi/vci*
21. **bridge-dot1q encap** *provider-vlan-id*
22. **encapsulation aal5snap**
23. **service-policy out egress-policy**
24. **pppoe-client dial-pool-number** *number*
25. **pppoe-client control-packets vlan cos** *number*
26. **service-policy input ingress-policy**
27. **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.

	Command or Action	Purpose
Step 3	**class-map match-all egress** **Example:** `Device(config)# class-map match-all egress`	Determines how packets are evaluated when multiple match criteria exist for the egress.
Step 4	**match qos-group** *number* **Example:** `Device(config)# match qos-group 101`	Identifies a specific quality of service (QoS) group value as a match criterion. The range is from 0 to 1023.
Step 5	**class-map match-all ingress** **Example:** `Device(config)# class-map match-all ingress`	Determines how packets are evaluated when multiple match criteria exist for the ingress.
Step 6	**match input-interface** *name* **Example:** `Device(config)# match input-interface Vlan2`	Configures a class map to use the specified input interface as a match criterion.
Step 7	**policy-map egress-policy** **Example:** `Device(config)# policy-map egress-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify an egress service policy and enters policy-map configuration mode.
Step 8	**class egress** **Example:** `Device(config-pmap)# class egress`	Specifies the name of the egress class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode.
Step 9	**set cos** *number* **Example:** `Device(config-pmap-c)# set cos 5`	Sets the CoS value. The range is from 0 to 7. **Note** The “set cos <value>” command marks the DOT1Q packets sent through the ATM interface with a cos(bitp) value over ATM AAL header. To set the “set cos <value>” command in action, a policy needs to be installed on the interface using the command “service-policy out <policy-name>”. Once the policy is enabled, the “set cos <value>” command attaches the specific cos value under the VLAN header. This feature is available from 17.7 release.
Step 10	**set vlan-inner** *number* **Example:** `Device(config-pmap-c)# set vlan-inner 333`	(For PPPoE) Sets the inner VLAN value. The range is from 1 to 4094.
Step 11	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.
Step 13	**policy-map ingress-policy** **Example:** `Device(config)# policy-map ingress-policy`	Creates or modifies a policy map that can be attached to one or more interfaces to specify an ingress service policy and enters policy-map configuration mode.
Step 14	**class ingress** **Example:** `Device(config-pmap)# class ingress`	Specifies the name of the ingress class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy. Enters policy-map class configuration mode
Step 15	**set qos-group** *number* **Example:** `Device(config-pmap-c)# set qos-group 101`	Sets the CoS value for a CoS group. The range is from 0 to 1023.
Step 16	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 17	**exit** **Example:** `Device(config-pmap)# exit`	Exits policy-map configuration mode and returns to global configuration mode.

Step 18	Enter one of the following:
	• **interface atm** *interface-id* **point-to-point**
	• **interface atm** *slot* **/ 0 point-to-point**
	• **interface atm** *slot/ port-adaptor*/**0 point-to-point**
	Example:
	`Device(config)# interface atm0 point-to-point`
	Example:
	`Device(config)# interface atm 0/0 point-to-point`
	Example:
	`Device(config)# interface atm 0/1/0.1 point-to-point`
		Specifies the ATM point-to-point interface using the appropriate format of the command and enters interface or subinterface configuration mode.

Step 19	**bridge-group** *group-number* **Example:** `Device(config-if)# bridge-group 1`	Assigns the interface or subinterface to a bridge group.
Step 20	**pvc** *vpi/vci* **Example:**	Creates a PVC of a specified virtual path identifier (VPI)/virtual circuit identifier (VCI) number and enters

	Command or Action	Purpose
	`Device(config-if)# pvc 9/117`	interface ATM VC configuration mode or subinterface ATM VC configuration mode.
Step 21	**bridge-dot1q encap** *provider-vlan-id* **Example:** `device(config-if-atm-vc)# bridge-dot1q encap`	Enables the router to include the 802.1Q VLAN ID in the MAC PDU. The service provider VLAN ID range is from 1 to 4094.
Step 22	**encapsulation aal5snap** **Example:** `Device(config-if-atm-vc)# encapsulation aal5snap`	Specifies the ATM Adaptation Layer 5 (AAL5) encapsulation type. AAL5SNAP is used so that two or more protocols can be multiplexed over the virtual circuit.
Step 23	**service-policy out egress-policy** **Example:** `Device(config-if-atm-vc)# service-policy out egress-policy`	Defines the service policy at the egress.
Step 24	**pppoe-client dial-pool-number** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures a PPP over Ethernet (PPPoE) client and specifies dial-on-demand routing (DDR) functionality.
Step 25	**pppoe-client control-packets vlan cos** *number* **Example:** `Device(config-if-atm-vc)# pppoe-client control-packets vlan cos 6`	Enables CoS marking for PPPoE control packets on the PPPoE client.
Step 26	**service-policy input ingress-policy** **Example:** `Device(config-if-atm-vc)# service-policy input ingress-policy`	Defines the service policy at the ingress.
Step 27	**end** **Example:** `Device(config-if-atm-vc)# end`	Exits interface ATM VC configuration mode, or subinterface ATM VC configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp authentication**
- **debug ppp negotiation**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**

- **debug aaa authorization**

Caution Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

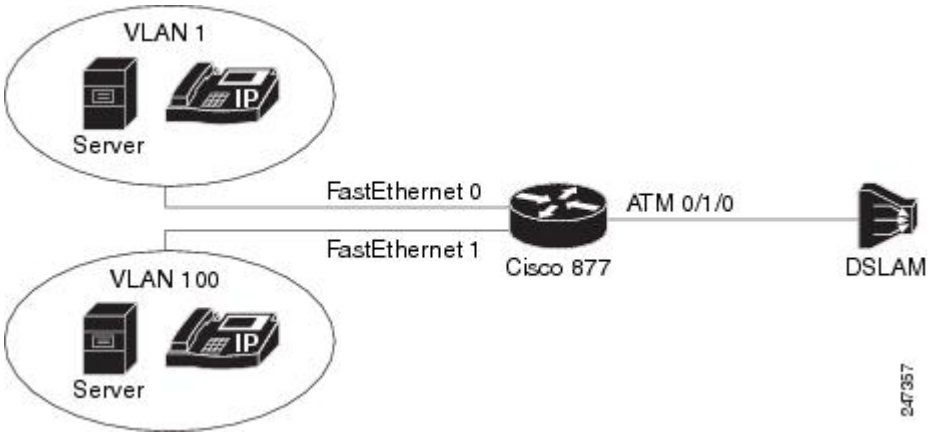
Configuration Examples for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Example: Traffic from Multiple Incoming VLANs Bridged to a VLAN

The following example shows how the traffic from multiple incoming VLANs is bridged to a single outgoing VLAN. The traffic arrives on Layer 2 Fast Ethernet ports and a DHCP server assigns IP addresses on the private network. Network Address Translation (NAT) is enabled. A static IP address is used on the outgoing Bridge-Group Virtual Interface (BVI) interface.

This topology is shown in the figure below.

Figure 9: Topology: Traffic from Multiple Incoming VLANs Bridged to a Single Outgoing VLAN



The following configuration is for the Cisco 877 router.

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
!
bridge irb
!
```

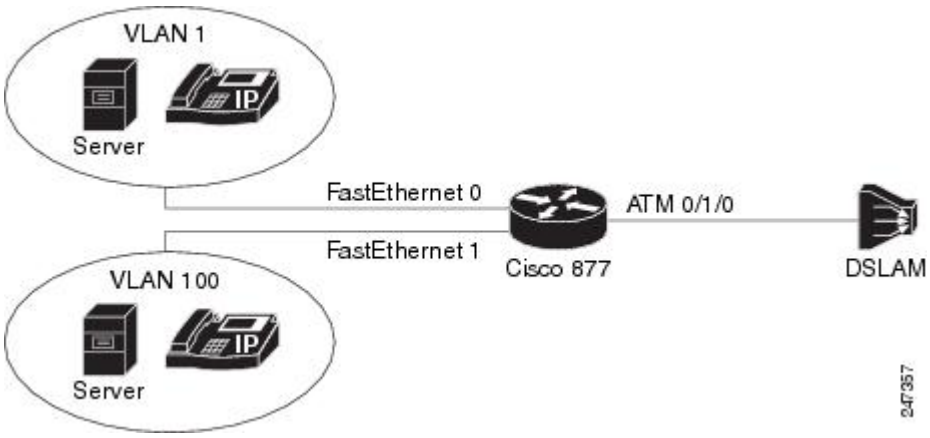
```
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 0/110
  bridge-dot1q encap 10
  encapsulation aal5snap
!
interface FastEthernet0
 switchport access vlan 1
!
interface FastEthernet1
 switchport access vlan 100
!
interface Vlan1
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Vlan100
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface BVI1
 ip address 10.0.0.0 255.0.0.0
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip nat pool test 10.0.0.0 10.0.0.0 netmask 255.0.0.0
ip nat inside source list 101 pool test overload
ip nat inside source list 102 pool test overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
!
```

Example: Traffic from Multiple VLANs Arrives at the Router over a Layer 3 Port

The following example shows how traffic from multiple VLANs arrives at the router over a Layer 3 port. All this traffic is bridged over a single ATM virtual circuit to the service provider's DSLAM and tagged with a single VLAN tag. Both WAN and LAN IP addresses are provided by DHCP servers.

This topology is shown in the figure below.

Figure 10: Topology: Traffic From Multiple VLANs Arrives at the Router over a Layer 3 Port



The following configuration is for the Cisco 877 router.

```
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool test_pool1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
ip dhcp pool test_pool2
   network 192.168.20.0 255.255.255.0
   default-router 192.168.20.1
!
bridge irb
!
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
 interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet0/1.2
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface ATM0/1/0
 no ip address
 no atm ilmi-keepalive
!
!
interface ATM0/1/0.1 point-to-point
 bridge-group 1
 bridge-group 1 spanning-disabled
 pvc 9/117
  bridge-dot1q encap 10
  encapsulation aal5snap
```

```
!
!
interface BVI1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
!
ip forward-protocol nd
!
ip nat inside source list 101 interface BVI1 overload
ip nat inside source list 102 interface BVI1 overload
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 any log
access-list 102 permit ip 192.168.20.0 0.0.0.255 any log
!
bridge 1 protocol ieee
bridge 1 route ip
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List , All Releases
ATM commands	Cisco IOS Asynchronous Transfer Mode Command Reference

Standards and RFCs

Standard/RFC	Title
IEEE 802.1P	*Traffic Class Expediting and Dynamic Multicast Filtering*
IEEE 802.1Q	*Virtual LANs*
IEEE 802.3	*LAN/MAN CSMA/CD (Ethernet) Access Method*
ITU-T G.992.1 (G.dmt)	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers*
ITU-T G.992.5	*Asymmetrical Digital Subscriber Line (ADSL) Transceivers-Extended Bandwidth ADSL2 (ADSL2+)*
ITU-T I363.5	*B-ISDN ATM Adaptation Layer Specification: Type 5 AAL*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 14: Feature Information for Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks

Feature Name	Releases	Feature Information
Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks	15.1(2)T	The Preserve 802.1Q Tagging with 802.1P Marking over ATM PVCs for xDSL Uplinks feature allows 802.1P marking based on 802.1Q tags and transportation of these tags over ATM PVC used in ADSL2+ uplinks. The following commands were introducef: **pppoe-client control-packets vlan cos**, **set vlan-inner**.
Transporting VLAN Tags over DSL Links	15.0(1)XA	The Transporting VLAN Tags over DSL Links feature allows 802.1Q tags to be transported over ATM PVCs used in ADSL2+ uplinks. The following command was introducef: **bridge-dot1q encap**.

Glossary

802.1ad—An amendment to IEEE 802.1Q that enables a service provider to offer bridged VLANs over its network.

802.1P—A 3-bit field within an Ethernet frame header added when using IEEE 802.1Q on an IEEE 802.1D network. It specifies a priority value from 0 and 7 that can be used by quality of service (QoS) disciplines to differentiate traffic.

802.1Q—A networking standard written by the IEEE 802.1 workgroup allowing multiple bridged networks to transparently share the same physical network link without leakage of information between networks. 802.1Q is commonly referred to as VLAN tagging.

AAL5SNAP—ATM Adaptation Layer 5 Subnetwork Protocol Access Protocol. A type of network encapsulation that supports multiplexing of two or more protocols over a virtual circuit.

ATM—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

BVI—Bridge Group Virtual Interface. A logical Layer 3-only interface associated with a bridge group when integrated bridging and routing (IRB) is configured.

CPE—Customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. This term can also refer to any telephone equipment residing on the customer site.

CVLAN—Customer Virtual Local Area Network.

DSL—Digital subscriber line. A public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL.

DSLAM—Digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

IRB—Integrated routing and bridging. Integrated Services Digital Network (ISDN) User Part. An upper-layer application supported by Signalling System 7 for connection setup and tear down.

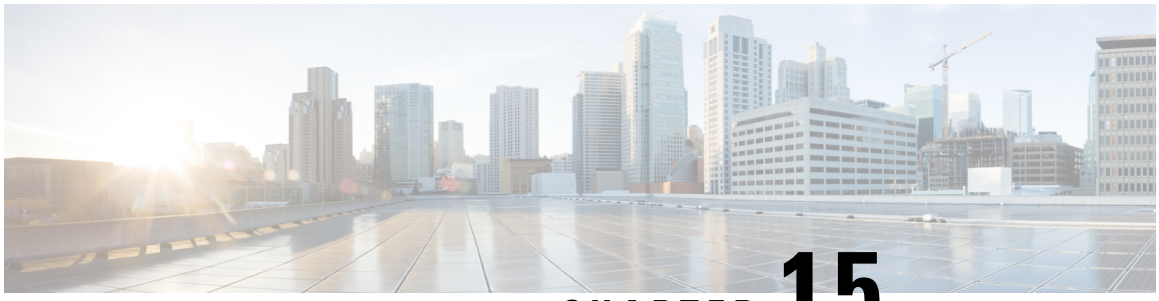
NAT—Network Address Translation. A mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

PVC—Permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, this is called a permanent virtual connection.

VoIP—Voice over IP. The capability to carry normal telephony-style voice over an IP-based Internet with plain old telephone service (POTS) like functionality, reliability, and voice quality.

PART II

Broadband Access Aggregation and DSL



CHAPTER 15

Preparing for Broadband Access Aggregation

Before you begin to perform the tasks required to accomplish broadband access aggregation, there are several preparatory tasks that you can perform at your option to enable you to complete the aggregation task with more efficiency. This module presents three of those preparation tasks: configuring permanent virtual circuits (PVCs), configuring a virtual template interface, and configuring enhancements for broadband scalability.

In a digital subscriber line (DSL) environment, many applications require the configuration of a large number of PVCs. Configuring PVCs before you start broadband aggregation can save you time because configuring a range of PVCs is faster than configuring PVCs individually.

A virtual template interface saves time because all PPP parameters are managed within the virtual template configuration. Any configurations made in the virtual template are automatically propagated to the individual virtual access interfaces.

Using the enhancement for broadband scalability reduces the amount of memory that is used per terminated PPP session by creating virtual access subinterfaces. Determining if virtual access subinterfaces are available on your system and preconfiguring these enhancements can speed your aggregation process and improve system performance.

Prerequisites for Preparing for Broadband Access Aggregation

Before configuring broadband access aggregation, you will need to know the information that is presented in the "Understanding Broadband Access Aggregation" module.

Additional information can be found in these documents:

- Configuring a PVC range--For detailed information about configuring individual ATM PVCs, see "Configuring PVCs" in the Cisco IOS Wide-Area Networking Configuration Guide.
- Creating a virtual template--For detailed information see the "Configuring Virtual Template Interfaces" chapter in the Cisco IOS Dial Technologies Configuration Guide.

Restrictions for Preparing for Broadband Access Aggregation

- Due to high scaling requirements, only virtual access subinterfaces are supported. Disabling virtual access subinterfaces is not supported.
- Precloning virtual access interfaces is not supported.
- When an interface has large number of subinterfaces disabled, the interface's Remote Access (RA) messages that have a lifetime value of zero are not sent to all its subinterfaces.

Information About Preparing for Broadband Access Aggregation

Virtual Access Interfaces

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

Once the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), and protocol translation.

All PPP parameters are managed within the virtual template configuration. Configuration changes made to the virtual template are automatically propagated to the individual virtual access interfaces. Multiple virtual access interfaces can originate from a single virtual template.

Cisco IOS XE software supports up to 4096 virtual template configurations. If greater numbers of tailored configurations are required, an authentication, authorization, and accounting (AAA) server can be used.

If the parameters of the virtual template are not explicitly defined before the interface is configured, the PPP interface is brought up using default values from the virtual template. Some parameters (such as an IP address) take effect only if specified before the PPP interface comes up. Therefore, it is recommended that you explicitly create and configure the virtual template before configuring the interface to ensure that such parameters take effect. Alternatively, if parameters are specified after the interface has been configured, use the **shutdown** command followed by the **no shutdown** command on the subinterface to restart the interface; this restart will cause the newly configured parameters (such as an IP address) to take effect.

Configuration Enhancements for Broadband Scalability

The Configuration Enhancements for Broadband Scalability feature reduces the amount of memory that is used per terminated PPP session by creating virtual-access subinterfaces. Depending on the configuration of the source virtual template, virtual-access subinterfaces may be available. This feature also introduces a command to determine if a virtual template is compatible with virtual access subinterfaces.

Virtual Access Subinterfaces

The **virtual-template** command supports existing features, functions, and configurations. By default, the **virtual-template subinterface** command is enabled; this command cannot be disabled.

The virtual template manager will determine if the set of options configured on the virtual template are all supported on a subinterface. Virtual access subinterfaces will be created for all virtual templates that support subinterfaces. If the user has entered any commands that are not supported on a subinterface, a full virtual access interface is created and cloned for all PPP sessions using that virtual template.

Different applications can use the same virtual template even if one application is subinterface-capable and another is not. The virtual template manager is notified whether the application supports virtual access subinterfaces and creates the appropriate resource.

Virtual Template Compatibility with Subinterfaces

The **test virtual-template subinterface** privileged EXEC command determines whether a virtual template can support the creation of a virtual access subinterface. If the virtual template contains commands that prevent the creation of subinterfaces, the **test virtual-template subinterface** command identifies and displays these commands.

The **debug vtemplate subinterface** command displays debug messages that are generated if you enter configuration commands on the virtual template that are not valid on a subinterface. These messages are generated only if the **debug vtemplate subinterface** command is enabled, the **virtual-template subinterface command** is enabled, and a virtual template is configured that can support the creation of subinterfaces. If the creation of virtual access subinterfaces is disabled by the **no virtual-template** subinterface command, the **debug vtemplate subinterface** command produces no output.

Benefits of Broadband Scalability Features

Using broadband scalability reduces the amount of memory that is used per terminated PPP session by creating virtual access subinterfaces. These virtual access subinterfaces, along with improvements that are transparent to the user, speed up the cloning process.

How to Prepare for Broadband Access Aggregation

Configuring a Virtual Template Interface

Configure a virtual template interface before you configure PPPoE on an Ethernet interface. The virtual template interface is a logical entity that is applied dynamically as needed to an incoming PPP session request. Perform this task to create and configure a virtual template interface:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **Interface virtual-template** *number* [**type** [**ethernet** | **serial** | **tunnel**]]
4. **ip unnumbered ethernet** *number*
5. **mtu** *bytes*
6. **ppp authentication chap**
7. **ppp ipcp ip address required**
8. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**Interface virtual-template** *number* [**type** [**ethernet** | **serial** | **tunnel**]] **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**ip unnumbered ethernet** *number* **Example:** `Router(config-if)# ip unnumbered ethernet 3/1`	Enables IP without assigning a specific IP address on the LAN.
Step 5	**mtu** *bytes* **Example:** `Router(config-if)# mtu bytes`	(Optional) Sets the maximum MTU size for the interface. • Valid range for the MTU size is 1492 or 1500.
Step 6	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 7	**ppp ipcp ip address required** **Example:** `Router(config-if)# ppp ipcp ip address required`	Prevents a PPP session from being set up without a valid address being negotiated. This command is required for legacy dialup and DSL networks.
Step 8	end **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Examples

The following example shows the configuration of a virtual template interface:

```
Router(config)# interface virtual-template 1
Router(config)# ip unnumbered21 Loopback1
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication chap
Router(config-if)# ppp authorization
Router(config-if)# ppp accounting
```

Configuring Enhancements for Broadband Scalability

To configure enhancement for broadband scalability, you will perform the following task:

Verifying Virtual Template Compatibility with Virtual Access Subinterfaces

Perform the following task to test a virtual template to determine if it is compatible with the creation of virtual access subinterfaces.

SUMMARY STEPS

1. **enable**
2. **test virtual-template** *template* **subinterface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**test virtual-template** *template* **subinterface** **Example:** `Router# test virtual-template virtual-template1 subinterface`	Tests the specified virtual template to determine if it is compatible with the creation of virtual access subinterfaces.

Examples

The output generated by the **test virtual-template subinterface** command describes the compatibility of the virtual template with the creation of subinterfaces.

This example shows output indicating that the virtual template is not compatible. This output also includes a list of the commands, which are configured on the virtual template, that cause the incompatibility.

```
Router# test virtual-template virtual-template1 subinterface

Subinterfaces cannot be created using
Virtual-Template1
Interface commands:
traffic-shape rate 50000 8000 8000 1000
```

Configuration Examples for Preparing for Broadband Access Aggregation

Virtual Access Subinterfaces Configuration Examples

This section provides the following configuration examples:

Virtual Access Subinterface Configuration Example

The example that follows shows a virtual template that is compatible with virtual access subinterfaces:

Note The **virtual-access subinterface** command is enabled by default and does not appear in running configurations. Only the **no virtual-access subinterface** command will appear in running configurations.

```
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pool-1
 ppp authentication chap
 ppp multilink
```

The following example shows a configuration in which the creation of virtual access subinterfaces has been disabled by the **no virtual-access subinterface** command. When this command is configured, virtual access interfaces are not registered with the SNMP code on the router. In network environments that do not use SNMP to manage PPP sessions, this saves the memory and CPU processing that would be used to register the virtual access interfaces with the SNMP code.

```
Current configuration :6003 bytes
!
! Last configuration change at 10:59:02 EDT Thu Sep 19 2004
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname ioswan5-lns
!
enable password lab
!
username cisco password 0 cisco
clock timezone EST -5
clock summer-time EDT recurring
aaa new-model
!
!
aaa authentication ppp default local
aaa authorization network default local
aaa session-id common
```

```
ip subnet-zero
no ip gratuitous-arps
ip cef
!
!
no ip domain lookup
ip name-server 10.44.11.21
ip name-server 10.44.11.206
!
ip vrf vpn1
rd 10:1
route-target export 10:1
route-target import 10:1
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname ioswan5-lac
local name tunnel1
l2tp tunnel password 7 01100F175804
!
!


!
no virtual-template subinterface
no virtual-template snmp
virtual-template 1 pre-clone 10
!
!
!
buffers small permanent 20000
buffers middle permanent 7500
!
!
!
interface Loopback1
ip address 10.111.1.1 255.255.255.0
```

Testing a Virtual Template for Compatibility with Subinterfaces Example

This example shows the process for testing a virtual template to determine if it can support virtual access subinterfaces. The following command displays the configuration for virtual template 1:

```
Router# show running interface virtual-template 1
Building configuration...
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool pool-1
ppp authentication chap
traffic-shape rate 50000 8000 8000 1000
end
```

The **test virtual-template subinterface** command tests virtual template 1 to determine if it can support subinterfaces. The output shows that the **traffic-shape rate** command that is configured on virtual template 1 prevents the virtual template from being able to support subinterfaces.

```
Router# test virtual-template 1 subinterface
Subinterfaces cannot be created using Virtual-Template1
Interface commands:
traffic-shape rate 50000 8000 8000 1000
```

Additional References

The following sections provide references related to preparing for broadband access aggregation.

Related Documents

Related Topic	Document Title
Broadband access aggregation of PPPoE Sessions	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions
Specifying a range for the ppp-max payload tag value	PPP-Max-Payload and IWF PPPoE Tag Support
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

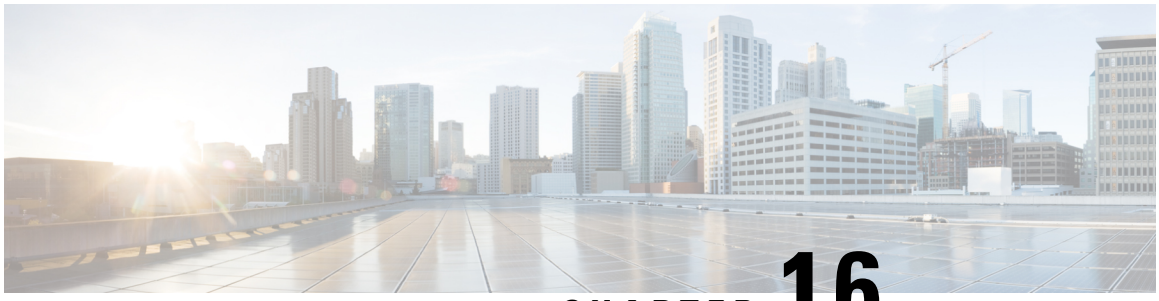
Feature Information for Preparing for Broadband Access Aggregation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 15: Feature Information for Preparing for Broadband Aggregation

Feature Name	Software Releases	Feature Configuration Information
Virtual Sub-Interface--Configuration Enhancements for Broadband Scalability	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. This feature reduces the amount of memory that is used per terminated PPP session by creating virtual access subinterfaces. Depending on the configuration of the source virtual template, virtual access subinterface may be available. This feature also introduces a command to determine if a virtual template is compatible with virtual access subinterfaces.



CHAPTER 16

Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

PPP over Ethernet profiles contain configuration information for a group of PPP over Ethernet (PPPoE) sessions. Multiple PPPoE profiles can be defined for a device, allowing different virtual templates and other PPPoE configuration parameters to be assigned to different PPP interfaces, VLANs, and ATM permanent virtual circuits (PVCs) that are used in supporting broadband access aggregation of PPPoE sessions.

Note This module describes the method for configuring PPPoE sessions using profiles.

Prerequisites for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

- You must understand the concepts described in the Understanding Broadband Access Aggregation module.
- You must perform the tasks contained in the Preparing for Broadband Access Aggregation module.

Restrictions for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

If a PPPoE profile is assigned to a PPPoE port (Gigabit Ethernet interface or PVC), virtual circuit (VC) class, or ATM PVC range and the profile has not yet been defined, the port, VC class, or range will not have any PPPoE parameters configured and will not use parameters from the global group.

The subscriber features that are supported/ not supported on PPP sessions are listed in the table below:

Table 16: Subscriber Features Supported and not Supported on PPP Sessions

Feature Name	Support Release
Per Subscriber Firewall on LNS	Cisco IOS XE Release 2.2.1. Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2
Per Subscriber Firewall on PTA	Not supported
Per Subscriber NAT	Support PPPoE with Carrier Grade NAT (CGN) in Cisco IOS XE Release 3.6
Per Subscriber PBR	Supports up to 1000 sessions from Cisco IOS XE Release 3.1S
Per Subscriber NBAR	Not supported
Per Subscriber Multicast	Supports up to 3,000 sessions from Cisco IOS XE Release 2.2.1 Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2
Per Subscriber Netflow	Not supported
Per Subscriber QPPB	Not supported
MLPPP on LNS, MLPoE on PTA, MLPoE LAC Switching	Supported. For more information see Configuring Multilink Point-to-Point Protocol Connections.
VLAN range	Not supported

Information About Providing Protocol Support for Broadband Access Aggregation for PPPoE Sessions

PPPoE Specification Definition

PPP over Ethernet (PPPoE) is a specification that defines how a host PC interacts with common broadband medium (for example, a digital subscriber line (DSL), wireless modem or cable modem) to achieve access to

a high-speed data network. Relying on two widely accepted standards, Gigabit Ethernet and PPP, the PPPoE implementation allows users over the Gigabit Ethernet to share a common connection. The Gigabit Ethernet principles supporting multiple users in a LAN, combined with the principles of PPP, which apply to serial connections, support this connection.

The base protocol is defined in RFC 2516.

PPPoE Connection Throttling

Repeated requests to initiate PPPoE sessions can adversely affect the performance of a router and RADIUS server. The PPPoE Connection Throttling feature limits PPPoE connection requests to help prevent intentional denial-of-service attacks and unintentional PPP authentication loops. This feature implements session throttling on the PPPoE server to limit the number of PPPoE session requests that can be initiated from a MAC address or VC during a specified period of time.

PPPoE VLAN Session Throttling

This feature throttles the number of PPPoE over QinQ sessions over each subinterface. If the number of new incoming session requests on the subinterface, exceeds the configured incoming session setup rate, the new session requests will be rejected. You can enable this capability independently on each Gigabit Ethernet subinterface.

The number of incoming session requests will be calculated separately on a combination of each port and subinterface, independent of each other. For example, if there are 2 subinterfaces sharing the QinQ VLAN IDs, the session rate of each is calculated separately. You should assign the bba-group configuration on each subscriber subinterface, with an unambiguous VLAN or outer and inner VLAN IDs (in the case of QinQ).

Autosense for ATM PVCs

The PPPoA/PPPoE Autosense for ATM PVCs feature enables a router to distinguish between incoming PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

Note The PPPoA/PPPoE Autosense for ATM PVCs feature is supported on Subnetwork Access Protocol (SNAP)-encapsulated ATM PVCs only. It is not supported on multiplexer (MUX)-encapsulated PVCs.

Benefits of Autosense for ATM PVCs

Autosense for ATM PVCs provides resource allocation on demand. For each PVC configured for PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoE session on that PVC. The autosense for ATM PVCs resources are allocated for PPPoE sessions only when a client initiates a session, thus reducing overhead on the NAS.

Note Autosense for ATM PVCs supports ATM PVCs only. Switched virtual circuits (SVCs) are not supported.

MAC Address for PPPoEoA

To prevent customers from experiencing unexpected behavior resulting from a system change, any change in the usage of MAC addresses will not happen unless it is explicitly configured.

Except for using a different MAC address, this feature does not change the way PPPoE works. This change is limited to ATM interfaces only--specifically, PPPoEoA--and will not be applied to other interfaces where PPPoE is operated on interfaces such as Gigabit Ethernet, Ethernet VLAN, and Data-over-Cable Service Interface Specifications (DOCSIS). Changing the PPPoE MAC address on those interfaces, which are broadcast in nature, requires placing the interface in promiscuous mode, thereby affecting the performance of the router because the router software has to receive all Gigabit Ethernet frames and then discard unneeded frames in the software driver.

This feature is disabled by default and applies to all PPPoE sessions on an ATM PVC interface configured in a BBA group.

When PPPoE and Rapid Bandwidth Expansion (RBE) are configured on two separate PVCs on the same DSL, the customer premises equipment (CPE) acts like a pure bridge, bridging from Gigabit Ethernet to the two ATM PVCs on the DSL. Because the CPE acts as a bridge, and because the aggregation router uses the same MAC address for both PPPoE and RBE, the CPE will not be able to bridge packets to the correct PVC. The solution is to have a different MAC address for PPPoE only. The MAC address can be either configured or selected automatically.

The MAC address of the PPPoEoA session is either the value configured on the ATM interface using the **mac-address** command or the burned-in MAC address if a MAC address is not already configured on the ATM interface. This functionality is effective only when neither autoselect nor a MAC address is specified on a broadband access group (BBA) group.

If the MAC address is specified on a BBA group, all PPPoEoA sessions use the MAC address specified on the BBA group, which is applied on the VC.

If the MAC address is selected automatically, 7 is added to the MAC address of the ATM interface.

Benefits of the Configurable MAC Address for PPPoE Feature

Because the Cisco IOS XE aggregation routers use the interface MAC address as the source MAC address for all broadband aggregation protocols on that interface, this feature solves problems that may occur when both RBE and PPPoE are deployed on the same ATM interface.

How to Provide Protocol Support for Broadband Access Aggregation of PPPoE Sessions

To provide protocol support for broadband access aggregation by assigning a profile, defining the profile is required.

When configuring a PPPoE session recovery after a system reload, perform the following task:

Defining a PPPoE Profile

Perform this task to define a PPPoE profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*]
6. **sessions per-mac limit** *per-mac-limit*
7. **sessions per-vlan limit** *per-vlan-limit* **inner** *per-inner-vlan-limit*
8. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
9. **sessions** {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period*
10. **ac name** *name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name*	**global**} **Example:** `Router(config)# bba-group pppoe global`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 8000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold at which an Simple Network Management Protocol (SNMP) trap will be generated. **Note** This command applies only to the global profile.
Step 6	**sessions per-mac limit** *per-mac-limit* **Example:**	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.

	Command or Action	Purpose
	`Router(config-bba-group)# sessions per-mac limit 2`	
Step 7	**sessions per-vlan limit** *per-vlan-limit* **inner** *per-inner-vlan-limit* **Example:** `Router(config-bba-group)# sessions per-vlan limit 200`	Sets the maximum number of PPPoE sessions permitted per VLAN in a PPPoE profile. • The **inner** keyword sets the number of sessions permitted per outer VLAN.
Step 8	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit 8`	Sets the maximum number of PPPoE sessions permitted on a VC in a PPPoE profile, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 9	**sessions** {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period* **Example:** `Router(config-bba-group)# sessions per-vc throttle 100 30 3008`	(Optional) Configures PPPoE connection throttling, which limits the number of PPPoE session requests that can be made from a VLAN, VC, or a MAC address within a specified period of time.
Step 10	**ac name** *name* **Example:** `Router(config-bba-group)# ac name ac1`	(Optional) Specifies the name of the access concentrator to be used in PPPoE active discovery offers (PADOs).
Step 11	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Exits BBA group configuration mode and returns to privileged EXEC mode.

Enabling PPPoE on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *number*
4. **encapsulation dot1q second-dot1q** {**any** \| *vlan-id*}
5. **pppoe enable** [**group** *group-name*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *number* **Example:** `Router(config)# interface gigabitethernet 0/0/0.0`	Specifies an Gigabit Ethernet interface and enters subinterface configuration mode.
Step 4	**encapsulation dot1q second-dot1q** {**any** | *vlan-id*} **Example:** `Router(config-subif)# encapsulation dot1q second-dot1q 1`	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
Step 5	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group one`	Enables PPPoE sessions on an Gigabit Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface by using the **group** *group-name* option, the interface will use the global PPPoE profile.
Step 6	**end** **Example:** `Router(config-subif)# end`	(Optional) Exits subinterface configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM PVC

Perform this task to assign a PPPoE profile to an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **pvc** *vpi* / *vci*
5. Do one of the following:
   - **protocol pppoe** [**group** *group-name*]
   - or
   - **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
6. **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 atm** *number* [**point-to-point** | **multipoint**] **Example:** `Device(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**pvc** *vpi* / *vci* **Example:** `Device(config-if)# pvc 2/101`	Creates an ATM PVC and enters ATM virtual circuit configuration mode.

Step 5	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	• or
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	Example:
	`Device(config-if-atm-vc)# protocol pppoe group one`
	Example:
	`or`
	Example:
	`Device(config-if-atm-vc)# encapsulation aal5autoppp virtual-template 1 group one`
		Enables PPPoE sessions to be established on ATM PVCs.
		or
		Configures PPPoE autosense on the PVC.
		Note If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

Step 6	**end** **Example:** `Device(config-if-atm-vc)# end`	(Optional) Exits ATM virtual circuit configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM PVC Range and PVC Within a Range

Perform this task to assign a PPPoE profile to an ATM PVC range and PVC within a range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **protocol pppoe** [**group** *group-name*]
6. **pvc-in-range** [*pvc-name*] [[*vpi* /]*vci*]
7. Do one of the following:
   - **protocol pppoe** [**group** *group-name*]
   - or
   - **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
8. **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 atm** *number* [**point-to-point**	**multipoint**] **Example:** `Device(config)# interface atm 5/1 multipoint`	Specifies an ATM interface and enters interface configuration mode.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Device(config-if)# range range-one pvc 100 4/199`	Defines a range of PVCs and enters ATM PVC range configuration mode.
Step 5	**protocol pppoe** [**group** *group-name*] **Example:** or **Example:** **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*] **Example:**	Enables PPPoE sessions to be established on a range of ATM PVCs. or Configures PPPoE autosense. **Note** If a PPPoE profile is not assigned to the PVC range by using the **group** *group-name* option, the PVCs in the range will use the global PPPoE profile.

	Command or Action	Purpose

	`Device(config-if-atm-range)# protocol pppoe group one`
	Example:
	or
	Example:
	`Device(config-if-atm-range)# encapsulation aal5autoppp virtual-template 1 group one`	

Step 6	**pvc-in-range** [*pvc-name*] [[*vpi* /]*vci*] **Example:** `Device(config-if-atm-range)# pvc-in-range pvc1 3/104`	Defines an individual PVC within a PVC range and enables ATM PVC-in-range configuration mode.

Step 7	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	• or
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	Example:
	`Device(config-if-atm-range-pvc)# protocol pppoe group two`
	Example:
	or
	Example:
	`Device(config-if-atm-range-pvc)# encapsulation aal5autoppp virtual-template 1 group two`
		Enables PPPoE sessions to be established on a PVC within a range.
		or
		Configures PPPoE autosense.
		Note If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

Step 8	**end** **Example:** `Device(cfg-if-atm-range-pvc)# end`	(Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM VC Class

Perform this task to assign a PPPoE profile to an ATM VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. Do one of the following:

- **protocol pppoe** [**group** *group-name*]
- or
- **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]

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	**vc-class atm** *vc-class-name* **Example:** `Device(config)# vc-class atm class1`	Creates an ATM VC class and enters ATM VC class configuration mode. • A VC class can be applied to an ATM interface, subinterface, or VC.

Step 4	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	• or
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	Example:
	`Device(config-vc-class)# protocol pppoe group two`
	Example:
	`Device(config-vc-class)# encapsulation aal5autoppp virtual-template 1 group two`
		Enables PPPoE sessions to be established.
		or
		Configures PPPoE autosense.
		Note If a PPPoE profile is not assigned by using the **group** *group-name* option, the PPPoE sessions will be established with the global PPPoE profile.

Step 5	**end** **Example:** `Device(config-vc-class)# end`	(Optional) Exits ATM VC class configuration mode and returns to privileged EXEC mode.

Configuring Different MAC Addresses on PPPoE

The Configurable MAC Address for PPPoE feature configures the MAC address on ATM PVCs in a broadband access (BBA) group to use a different MAC address for PPP over Ethernet over ATM (PPPoEoA).

Perform this task to configure different MAC addresses on PPPoE and enable the aggregation device to bridge packets from Gigabit Ethernet to the appropriate PVC.

Before you begin

A BBA group profile should already exist. The BBA group commands are used to configure broadband access on aggregation and client devices that use PPPoE, and routed bridge encapsulation (RBE).

Perform this task to configure different MAC addresses on PPPoE and enable the aggregation device to bridge packets from Gigabit Ethernet to the appropriate PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*bba-group-name* | **global**}
4. **mac-address** {**autoselect** | *mac-address*}
5. **end**
6. **show pppoe session**

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	**bba-group pppoe** {*bba-group-name*	**global**} **Example:** `Device(config)#bba-group pppoe group1`	Enters BBA group configuration mode.
Step 4	**mac-address** {**autoselect**	*mac-address*} **Example:** `Device(config-bba-group)# mac-address autoselect`	Selects the MAC address, as follows: • **autoselect** --Automatically selects the MAC address based on the ATM interface address, plus 7. • *mac-address* --Standardized data link layer address having a 48-bit MAC address. Also known as a hardware address, MAC layer address, and physical address. All PPPoEoA sessions use the MAC address specified on the BBA group, which are applied on the VC.
Step 5	**end** **Example:** `Device(config-bba-group)# end`	Exits BBA group configuration mode.

	Command or Action	Purpose
Step 6	**show pppoe session** **Example:** `Device# show pppoe session`	Displays the MAC address as the local MAC (LocMac) address on the last line of the display.

Examples

The following example displays the MAC address as LocMac:

```
Device# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
     1 session total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      3      3  000b.fdc9.0001  ATM3/0.1                 1  Vi2.1
PTA
                0008.7c55.a054  VC:  1/50                   UP
LocMAC is burned in mac-address of ATM interface(0008.7c55.a054).
```

Configuring PPPoE Session Recovery After Reload

Perform this task to configure the aggregation device to send PPPoE active discovery terminate (PADT) packets to the CPE device upon receipt of PPPoE packets on "half-active" PPPoE sessions (a PPPoE session that is active on the CPE end only).

If the PPP keepalive mechanism is disabled on a customer premises equipment (CPE) device, a PPP over Ethernet (PPPoE) session will hang indefinitely after an aggregation device reload. The PPPoE Session Recovery After Reload feature enables the aggregation device to attempt to recover PPPoE sessions that failed because of reload by notifying CPE devices about the PPPoE session failures.

The PPPoE protocol relies on the PPP keepalive mechanism to detect link or peer device failures. If PPP detects a failure, it terminates the PPPoE session. If the PPP keepalive mechanism is disabled on a CPE device, the CPE device has no way to detect link or peer device failures over PPPoE connections. When an aggregation device that serves as the PPPoE session endpoint reloads, the CPE device will not detect the connection failure and will continue to send traffic to the aggregation device. The aggregation device will drop the traffic for the failed PPPoE session.

The **sessions auto cleanup** command enables an aggregation device to attempt to recover PPPoE sessions that existed before a reload. When the aggregation device detects a PPPoE packet for a half-active PPPoE session, the device notifies the CPE of the PPPoE session failure by sending a PPPoE PADT packet. The CPE device is expected to respond to the PADT packet by taking failure recovery action.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **sessions auto cleanup**
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	**bba-group pppoe** {*group-name* | **global**} **Example:** `Device(config)# bba-group pppoe global`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that will serve as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**sessions auto cleanup** **Example:** `Device(config-bba-group)# sessions auto cleanup`	Configures an aggregation device to attempt to recover PPPoE sessions that failed because of reload by notifying CPE devices about the PPPoE session failures.
Step 5	**end** **Example:** `Device(config-bba-group)# end`	(Optional) Exits BBA group configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **show pppoe session** and **debug pppoe** commands to troubleshoot PPPoE sessions.

Monitoring and Maintaining PPPoE Profiles

SUMMARY STEPS

1. **enable**
2. **show pppoe session** [**all** | **packets**]
3. **clear pppoe** {**interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] | **rmac** *mac-addr* [**sid** *session-id*] | **all**}
4. **debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}]]

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**show pppoe session** [**all** | **packets**] **Example:** `Device# show pppoe session all`	Displays information about active PPPoE sessions.
Step 3	**clear pppoe** {**interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] | **rmac** *mac-addr* [**sid** *session-id*] | **all**} **Example:** `Device# clear pppoe interface atm 0/0/0.0`	Terminates PPPoE sessions.
Step 4	**debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}]] **Example:** `Device# debug pppoe events`	Displays debugging information for PPPoE sessions.

Configuration Examples for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Example: PPPoE Profiles Configuration

The following example shows the configuration of three PPPoE profiles: vpn1, vpn2, and a global PPPoE profile. The profiles vpn1 and vpn2 are assigned to PVCs, VC classes, VLANs, and PVC ranges. Any Gigabit Ethernet interface, VLAN, PVC, PVC range, or VC class that is configured for PPPoE but is not assigned either profile vpn1 or vpn (such as VC class class-pppoe-global) will use the global profile.

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
 sessions per-mac limit 2
bba-group pppoe group1
 virtual-template 1
 sessions per-vlan throttle 1 10 50
!
interface GigabitEthernet5/0/0.2
 encapsulation dot1Q 20 second-dot1q 201
 pppoe enable group group1
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
```

```
 sessions per-mac limit 1 !
vc-class atm class-pppoe-global
 protocol pppoe
!
vc-class atm class-pppox-auto
 encapsulation aal5autoppp virtual-template 1 group vpn1
!
vc-class atm class-pppoe-1
 protocol pppoe group vpn1
!
vc-class atm class-pppoe-2
 protocol pppoe group vpn2
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
 !
interface ATM1/0.20 multipoint
 class-int class-pppox-auto
 pvc 0/200
  encapsulation aal5autoppp virtual-template 1
 !
 pvc 0/201
 !
 pvc 0/202
  encapsulation aal5autoppp virtual-template 1 group vpn2
 !
 pvc 0/203
  class-vc class-pppoe-global
 !
!
interface gigabitEthernet0/2/3.1
 encapsulation dot1Q 4
 pppoe enable group vpn1
!
interface gigabitEthernet0/2/3.2
 encapsulation dot1Q 2
 pppoe enable group vpn2
!
interface ATM0/6/0.101 point-to-point
 ip address 10.12.1.63 255.255.255.0
 pvc 0/101
 !
interface ATM0/6/0.102 point-to-point
 ip address 10.12.2.63 255.255.255.0
 pvc 0/102
 !
interface Virtual-Template1
 ip unnumbered loopback 1
 no logging event link-status
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered loopback 1
no logging event link-status
 no keepalive
 peer default ip address pool pool-2
 ppp authentication chap
!
```

```
ip local pool pool-1 198.x.1.z 198.x.1.y
ip local pool pool-2 198.x.2.z 198.x.2.y
!
```

Example: MAC Address of the PPPoEoA Session as the Burned-In MAC Address

In the following example, neither address autoselect nor a MAC address is configured on the BBA group. The MAC address is not configured on the ATM interface (the default condition). The **show pppoe session** command is used to confirm that the MAC address of the PPPoEoA session is the burned-in MAC address of the ATM interface.

```
bba-group pppoe one
 virtual-template 1
interface ATM0/3/0.0
 no ip address
 no ip route-cache
no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one
 !
Router# show pppoe session
1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      3      3  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0008.7c55.a054  VC:  1/50                  UP
LocMAC is burned in mac-address of ATM interface(0008.7c55.a054).
```

Example Address Autoselect Configured and MAC Address Not Configured

In the following example, address autoselect is configured on the BBA group, and the MAC address is not configured on the ATM interface. The **show pppoe session** command displays the MAC address of the interface, plus 7.

```
bba-group pppoe one
 virtual-template 1
 mac-address autoselect
!
interface ATM3/0
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
```

```
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                     VA-st
      5      5  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0008.7c55.a05b  VC:  1/50                  UP
LocMAC = burned in mac-address of ATM interface + 7 (0008.7c55.a05b)
```

Example: MAC Address Configured on the ATM Interface

In the following example, neither autoselect nor the MAC address is configured on the BBA group, but the MAC address is configured on the ATM interface, as indicated by the report from the **show pppoe session** command:

```
bba-group pppoe one
 virtual-template 1
interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
protocol pppoe group one
 !
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                     VA-st
      7      7  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0001.0001.0001  VC:  1/50                  UP
LocMAC = configured mac-address on atm interface(0001.0001.0001).
```

Example: MAC Address Configured on the BBA Group

In the following example, the MAC address is configured on the BBA group. The display from the **show pppoe session** command indicates that all PPPoEoA sessions on the ATM interface associated with the BBA group use the same MAC address as specified on the BBA group.

```
bba-group pppoe one
 virtual-template 1
 mac-address 0002.0002.0002
interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
```

```
  protocol pppoe group one
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                     VA-st
      8      8  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0002.0002.0002  VC:  1/50                  UP
LocMac(Mac address of PPPoEoA session) is mac-address specified on bba-group one
(0002.0002.0002)
```

Example: PPPoE Session Recovery After Reload

In the following example, the router attempts to recover failed PPPoE sessions on PVCs in the range-pppoe-1 ATM PVC range.

```
bba-group pppoe group1
 virtual-template 1
 sessions auto cleanup
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group group1
!
interface virtual-template1
 ip address negotiated
 no peer default ip address
 ppp authentication chap
```

Where to Go Next

- If you want to establish PPPoE session limits for sessions on a specific permanent virtual circuit or VLAN configured on an Layer Two Tunneling Protocol (L2TP) access concentrator, see the Establishing PPPoE Session Limits per NAS Port module.
- If you want to use service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup, see the Offering PPPoE Clients a Selection of Services During Call Setup module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to an L2TP network server (LNS) or tunnel switch, see the Enabling PPPoE Relay Discovery and Service Selection Functionality module.
- If you want to configure the transfer upstream of the PPPoX session speed value, see the Configuring Upstream Connections Speed Transfer module.
- If you want to use SNMP to monitor PPPoE sessions, see the Monitoring PPPoE Sessions with SNMP module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, see the Identifying a Physical Subscriber Line for RADIUS Access and Accounting module.
- If you want to configure a Cisco Subscriber Service Switch, see the Configuring Cisco Subscriber Service Switch Policies module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband and DSL commands	Broadband Access Aggregation and DSL Command Reference
Broadband access aggregation concepts	*Understanding Broadband Access Aggregation*
Tasks for preparing for broadband access aggregation.	*Preparing for Broadband Access Aggregation module*
Establishing PPPoE session limits for sessions on a specific permanent virtual circuit or VLAN configured on an Layer Two Tunneling Protocol (L2TP) access concentrator	*Establishing PPPoE Session Limits per NAS Port*
Using service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup	*Offering PPPoE Clients a Selection of Services During Call Setup*
Enabling an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to an L2TP network server (LNS) or tunnel switch	*Enabling PPPoE Relay Discovery and Service Selection Functionality*
Configuring the transfer upstream of the PPPoX session speed value	*Configuring Upstream Connections Speed Transfer*
Using SNMP to monitor PPPoE sessions	*Monitoring PPPoE Sessions with SNMP*
Identifying a physical subscribe line for RADIUS communication with a RADIUS server	I*dentifying a Physical Subscriber Line for RADIUS Access and Accounting*
Configuring a Cisco Subscriber Service Switch	*Configuring ISG Policies for Automatic Subscriber Logon*

Standards/RFCs

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5

Standards	Title
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

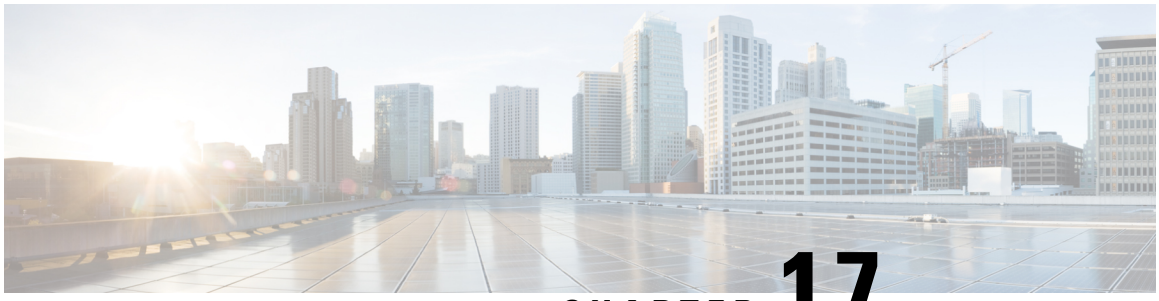
Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 17: Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Feature Name	Releases	Feature Information
PPPoE Connection Throttling	Cisco IOS XE Release 2.1	The PPPoE Connection Throttling feature limits PPPoE connection requests to help prevent intentional denial-of-service attacks and unintentional PPP authentication loops. This feature implements session throttling on the PPPoE server to limit the number of PPPoE session requests that can be initiated from a MAC address or virtual circuit during a specified period of time.
PPPoE Server Restructuring and PPPoE Profiles	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
PPPoE VLAN Session Throttling	Cisco IOS XE Release 2.4	This feature allows for PPPoE VLAN Session throttling support.



CHAPTER 17

PPP for IPv6

Information About PPP for IPv6

Accounting Start and Stop Messages

PPP calls a registry to allow DHCPv6 to append the delegated prefix information to accounting start and stop messages. When accounting is configured for a DHCPv6 pool, accounting interim packets are sent to broadband sessions after binding is provided from the pool.

Forced Release of a Binding

The DHCPv6 server maintains an automatic binding table in memory to track the assignment of some configuration parameters, such as prefixes between the server and its clients. The automatic bindings can be stored permanently in the database agent, which can be, for example, a remote TFTP server or local NVRAM file system.

DHCPv6 invokes a routine when the virtual interface used by PPP terminates. This routine automatically releases any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

When a PPP virtual interface terminates, the routine runs through the full table of DHCPv6 bindings checking for the matching interface. Because PPP uses a virtual interface, this subroutine clears any related lease information when the PPP connection terminates.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using the **ipv6 dhcp binding track ppp** command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

Delegated-IPv6-Prefix

The Delegated-IPv6-Prefix attribute calls DHCPv6 to parse and store AAA attribute information. PPP sends the accounting start and stop messages for PPP sessions.

The following is an example of a Delegated-IPv6-Prefix attribute:

cisco-avpair = ipv6:delegated-prefix=2001:DB8::/64

Note The Delegated-IPv6-Prefix attribute does not support the Cisco VSA format. If you try add this attribute in the cisco-vsa format in the profile, the RADIUS server response fails. Use only the IETF attribute for Delegated-IPv6-Prefix.

PPP IPv6 Accounting Delay Enhancements

This feature enhances accounting records for dual-stack networks. It ensures that a unique IPv6 address is assigned to PPP IPv6 and IPv4 sessions for IP addresses that are received from RADIUS.

When this feature is enabled, it automatically creates a database to hold new incoming access-accept responses from RADIUS. The access-accept responses in this database are then checked for duplicates of a specific set of attributes. If the attributes are already present in the database, then the RADIUS server has already offered them to an existing session; therefore, the new session is immediately removed and a stop-record message sent. If none of the specific set of attributes are in the database, they are immediately added to the database, and the session proceeds normally. When the session is removed, the entries in the database are also removed.

The following RADIUS attributes are tracked in the database and checked at access-accept time:

- Framed-IPv6-Prefix
- Delegated-IPv6-Prefix

The attributes are available as standard RFC-defined binary format, or as Cisco VSAs. (The Delegated-IPv6-Prefix attribute currently does not have a VSA definition in AAA.)

How to Configure PPP for IPv6

Enabling the Sending of Accounting Start and Stop Messages

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **accounting** *mlist*

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	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
Step 4	**accounting** *mlist* **Example:** `Device(config-dhcp)# accounting list1`	Enables accounting start and stop messages to be sent.

Removing Delegated Prefix Bindings

Perform this task to release any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp bindings track ppp**

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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface VirtualAccess2.2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 dhcp bindings track ppp** **Example:** `Device(config-if)# ipv6 dhcp bindings track ppp`	Releases any delegated prefix leases associated with the PPP virtual interface that is being terminated.

Configuring PPP IPv6 Accounting Delay Enhancements

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ppp unique address access-accept**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ppp unique address access-accept** **Example:** `Router(config)# ppp unique address access-accept`	Tracks duplicate addresses received from RADIUS and creates a standalone database.

Configuration Examples for PPP for IPv6

Example: Enabling the Sending of Accounting Start and Stop Messages

This example shows how to enable a device to send accounting start and stop messages.

```
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcp)# accounting list1
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco_IOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

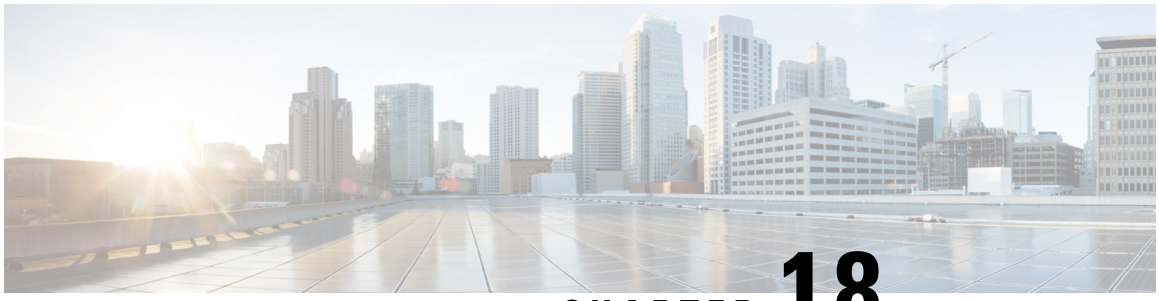
Feature Information for PPP for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 18: Feature Information for PPP for IPv6

Feature Name	Releases	Feature Information
PPP Enhancement for Broadband IPv6	Cisco IOS XE Release 2.5	IPv6 supports this feature. The following commands were introduced or modified: **accounting**, **ipv6 dhcp bindings track ppp**, **ipv6 dhcp pool**.
PPP IPv6 Accounting Delay Enhancements	Cisco IOS XE Release 3.2S	IPv6 supports this feature. The following commands were introduced or modified: **ppp unique address accept-access**.
SSO/ISSU Support for Per-User IPv6 ACL for PPP Sessions	Cisco IOS XE Release 3.2.1S	IPv6 supports this feature. No commands were introduced or modified.



CHAPTER 18

DHCP for IPv6 Broadband

The DHCP for IPv6 Broadband feature highlights the DHCP enhancements that support IPv6 broadband deployments. This feature briefly explains the different ways a delegating device selects prefixes for a requesting device, enabling accounting messages on a device, and forced release of delegated prefix bindings associated with a PPP virtual interface when the PPP virtual interface is terminated.

Information About DHCP for IPv6 Broadband

Prefix Delegation

An IPv6 prefix delegating device selects IPv6 prefixes to be assigned to a requesting device upon receiving a request from the client. The delegating device might select prefixes for a requesting device in the following ways:

- Dynamic assignment from a pool of available prefixes.
- Dynamic assignment from a pool name obtained from the RADIUS server.
- Assignment of prefix obtained from the RADIUS sever.

Contrary to IPv4 address assignment, an IPv6 user will be assigned a prefix, not a single address. Typically the Internet service provider (ISP) assigns a 64- or 48-bit prefix.

Accounting Start and Stop Messages

PPP calls a registry to allow DHCPv6 to append the delegated prefix information to accounting start and stop messages. When accounting is configured for a DHCPv6 pool, accounting interim packets are sent to broadband sessions after binding is provided from the pool.

Forced Release of a Binding

The DHCPv6 server maintains an automatic binding table in memory to track the assignment of some configuration parameters, such as prefixes between the server and its clients. The automatic bindings can be

stored permanently in the database agent, which can be, for example, a remote TFTP server or local NVRAM file system.

DHCPv6 invokes a routine when the virtual interface used by PPP terminates. This routine automatically releases any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

When a PPP virtual interface terminates, the routine runs through the full table of DHCPv6 bindings checking for the matching interface. Because PPP uses a virtual interface, this subroutine clears any related lease information when the PPP connection terminates.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using the **ipv6 dhcp binding track ppp** command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

How to Configure DHCP for IPv6 Broadband

Enabling the Sending of Accounting Start and Stop Messages

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **accounting** *mlist*

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	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

	Command or Action	Purpose
Step 4	**accounting** *mlist* **Example:** `Device(config-dhcp)# accounting list1`	Enables accounting start and stop messages to be sent.

Removing Delegated Prefix Bindings

Perform this task to release any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp bindings track ppp**

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** *type number* **Example:** `Device(config)# interface VirtualAccess2.2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 dhcp bindings track ppp** **Example:** `Device(config-if)# ipv6 dhcp bindings track ppp`	Releases any delegated prefix leases associated with the PPP virtual interface that is being terminated.

Configuration Examples for DHCP for IPv6 Broadband

Enabling the Sending of Accounting Start and Stop Messages

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **accounting** *mlist*

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	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
Step 4	**accounting** *mlist* **Example:** `Device(config-dhcp)# accounting list1`	Enables accounting start and stop messages to be sent.

Example: Configuration for a Prefix Allocated from a Local Pool

DHCPv6 clients are connected to the DHCPv6 server on Gigabit Ethernet interface 0/0/0. The server is configured to use parameters from the DHCP pool called dhcp-pool. This pool provides clients with the IPv6 address of a DNS server and the domain name to be used. It also specifies that prefixes can be delegated from the prefix pool called client-prefix-pool1. The prefixes delegated will have valid and preferred lifetimes of 1800 and 600 seconds respectively. The prefix pool named client-prefix-pool1 has a prefix of length /40 from which it will delegate (sub) prefixes of length /48.

```
ipv6 dhcp pool dhcp-pool
```

```
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface GigabitEthernet0/0/0
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
```

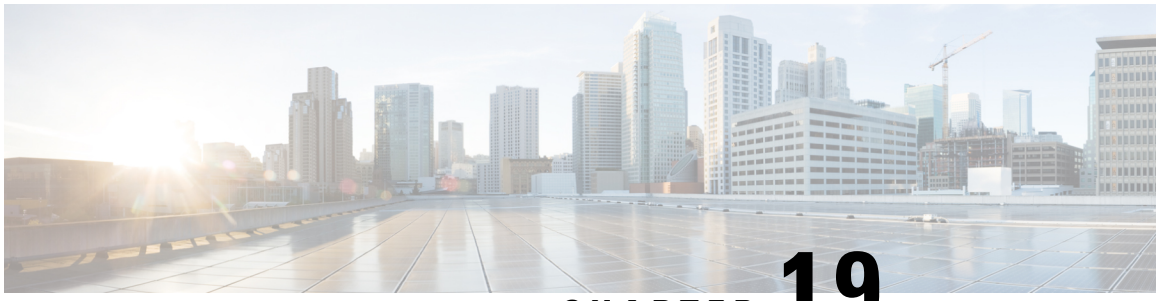
Feature Information for DHCP for IPv6 Broadband

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 19: Feature Information for DHCP for IPv6 Broadband

Feature Name	Releases	Feature Information
DHCP Enhancements to Support IPv6 Broadband Deployments	Cisco IOS XE Release 2.5	The feature highlights the DHCP enhancements that support IPv6 broadband deployments, such as, the different ways a delegating device selects prefixes for a requesting device, enabling accounting messages on a device, and forced release of delegated prefix bindings associated with a PPP virtual interface when the PPP virtual interface is terminated. The following commands were introduced or modified: **accounting**, **ipv6 dhcp bindings track ppp**, **ipv6 dhcp pool**.
DHCPv6 Prefix Delegation RADIUS VSA	Cisco IOS XE Release 2.5	When the user requests a prefix from the prefix delegator, typically the NAS, the prefix is allocated using DHCPv6.
DHCP Accounting Attribute	Cisco IOS XE Release 3.13S	The DHCP Accounting Attribute feature allows DHCPv6 to append delegated prefix information to accounting start and stop messages.



CHAPTER 19

Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

PPP over ATM enables a high-capacity central site router with an ATM interface to terminate multiple remote Point-to-Point Protocol (PPP) connections. PPP over ATM provides security validation per user, IP address pooling, and service selection capability.

Prerequisites for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Perform the preparation tasks in the "Preparing for Broadband Access Aggregation" module.

Restrictions for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

PPP over ATM cannot be configured on IETF-compliant Logical Link Control (LLC) encapsulated PPP over ATM.

Information About Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Virtual Access Interface

When you configure PPP over ATM, a logical interface known as a *virtual access interface* associates each PPP connection with an ATM virtual circuit (VC). You can create this logical interface by configuring an ATM permanent virtual circuit (PVC) or switched virtual circuit (SVC). This configuration encapsulates each PPP connection in a separate PVC or SVC, thus allowing each PPP connection to terminate at the ATM interface of a device as if received from a typical PPP serial interface.

After you have configured the device for PPP over ATM, the PPP subsystem starts and the device attempts to send a PPP configuration request to the remote peer. If the peer does not respond, the router periodically goes into a listen state and waits for a configuration request from the peer.

Before you create the ATM VC, we recommend that you create and configure a virtual template as described in the "Preparing for Broadband Access Aggregation" module. When the VC is created, the virtual access interface for each VC obtains the configuration from a virtual interface template (virtual template) .

The virtual access interface is associated with the VC after the completion of the LCP negotiation. When the PPP session goes down, the virtual access interface is no longer associated with the VC and is returned to the pool of free virtual-access interfaces.

If you set a keepalive timer of the virtual template on the interface, the virtual access interface uses the PPP echo mechanism to verify the existence of the remote peer.

The following types of PPP over ATM connections are supported:

- IETF-compliant Multiplex (MUX) encapsulated PPP over ATM
- IETF-compliant LLC encapsulated PPP over ATM

How to Provide Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Configuring IETF-Compliant MUX Encapsulated PPP over ATM on Point-to-Point Subinterface

Internet Engineering Task Force (IETF)-compliant multiplexer (MUX) encapsulated PPP over ATM, also known as *null encapsulation* , allows you to configure PPP over ATM using a VC multiplexed encapsulation mode. This feature complies with IETF RFC 2364 entitled PPP over AAL5.

You can configure ATM PVCs for IETF-compliant MUX encapsulated PPP over ATM on either point-to-point or multipoint subinterfaces.

Perform this task to configure IETF-compliant MUX Encapsulated PPP over ATM point-to-point subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number.subinterface-number* **point-to-point**
4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   -
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **encapsulation aal5mux ppp virtual-template** *number*
6. Do one of the following:
   - **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 atm** *number.subinterface-number* **point-to-point** **Example:** `Device(config)# interface atm 1.0 point-to-point`	Specifies the ATM point-to-point subinterface using the appropriate form of the **interface atm**command[7] and enters subinterface configuration mode.

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	Example:
	`Device(config-subif)# pvc cisco 0/5`
	Example:
	`or`
	Example:
		Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.

	Command or Action	Purpose
	`Device(config-subif)# range range1 pvc 1/200 1/299`	

Step 5	**encapsulation aal5mux ppp virtual-template** *number*
	Example:
	`Device(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3`
	Example:
	`or`
	Example:
	`Device(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3`
		Configures VC multiplexed encapsulation on a PVC or PVC range.

Step 6	Do one of the following:
	• **end**
	Example:
	`Device(config-subif-atm-vc)# end`
	Example:
	`or`
	Example:
	`Device(config-subif-atm-range)# end`
		Exits ATM virtual circuit range subinterface configuration mode.
		or
		Exits ATM range subinterface configuration mode.

Configuring IETF-Compliant MUX Encapsulated PPP over ATM on a Multipoint Subinterface

Multiple PVCs on multipoint subinterfaces significantly increase the maximum number of PPP-over-ATM sessions running on a device. You can configure IETF-compliant MUX encapsulated PPP over ATM on a single ATM PVC or an ATM PVC range.

Perform this task to configure IETF-compliant MUX Encapsulated PPP over ATM on a multipoint subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number.subinterface-number* **multipoint**
4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   -

- **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*

5. **encapsulation aal5mux ppp virtual-template** *number*
6. Do one of the following:
   - **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 atm** *number.subinterface-number* **multipoint** **Example:** `Device(config)# interface atm 1/0/0.4 multipoint`	Specifies the ATM multipoint subinterface using the appropriate form of the **interface atm**command and enters subinterface configuration mode.

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	Example:
	`Device(config-subif)# pvc cisco 0/5`
	Example:
	`or`
	Example:
	`Device(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.

Step 5	**encapsulation aal5mux ppp virtual-template** *number* **Example:** `Device(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3` **Example:**	Configures VC multiplexed encapsulation on a PVC or PVC range.

	Command or Action	Purpose
	or **Example:** `Device(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3`	

Step 6	Do one of the following:
	• **end**
	Example:
	`Device(config-subif-atm-vc)# end`
	Example:
	Example:
	`Device(config-subif-atm-range)# end`
		Exits ATM virtual circuit subinterface configuration mode.
		or
		Exits ATM range subinterface configuration mode.

Configuring IETF-Compliant LLC Encapsulated PPP over ATM on a Point-to-point Subinterface

IETF-compliant LLC encapsulated PPP over ATM allows you to configure PPP over ATM with LLC encapsulation. It accommodates Frame Relay-to-ATM service interworking (Frame Relay Forum standard FRF.8). There is no equivalent VC multiplexed encapsulation mode for Frame Relay; therefore, LLC encapsulation is required for Frame Relay-to-ATM networking. This version of PPP over ATM also enables you to carry multiprotocol traffic. For example, a VC will carry both PPP and IPX traffic.

The figure below shows Frame Relay-to-ATM interworking.

Figure 11: Frame Relay-to-ATM Interworking

You can configure ATM PVCs for IETF-compliant LLC encapsulated PPP over ATM on either point-to-point or multipoint subinterfaces. Multiple PVCs on multipoint subinterfaces significantly increase the maximum number of PPP-over-ATM sessions running on a router.

Perform this task to configure IETF-compliant LLC encapsulated PPP over ATM PVC or range of PVCs on a point-to-point interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number.subinterface-number* **point-to-point**

4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   -
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **encapsulation aal15snap**
6. **protocol ppp virtual-template** *number*
7. Do one of the following:
   - **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number.subinterface-number* **point-to-point** **Example:** `Router(config)# interface atm 6.200 point-to-point`	Specifies the ATM point-to-point or multipoint subinterface using the appropriate form of the **interface atm** command[8] and enters subinterface configuration mode.

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	Example:
	`Router(config-subif)# pvc cisco 0/5`
	Example:
	`or`
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.

	Command or Action	Purpose

Step 5	**encapsulation aal15snap**
	Example:
	`Router(config-subif-atm-vc)# encapsulation aal15snap`
	Example:
	`or`
	Example:
	`Router(config-subif-atm-range)# encapsulation aal15snap`
		Configures LLC SNAP encapsulation on the PVC or a range of PVCs.[9]

Step 6	**protocol ppp virtual-template** *number*
	Example:
	`Router(config-subif-atm-vc)# protocol ppp virtual-template 2`
	Example:
	`or`
	Example:
	`Router(config-subif-atm-range)# protocol ppp virtual-template 2`
		Configures IETF PPP over ATM LLC encapsulation on the PVC or a range of PVCs.

Step 7	Do one of the following:
	• **end**
	Example:
	`Router(config-subif-atm-vc)# end`
	Example:
	`or`
	Example:
	`Router(config-subif-atm-range)# end`
		Exits ATM virtual circuit subinterface configuration mode.
		or
		Exits ATM range subinterface configuration mode.

Configuring IETF-Compliant LLC Encapsulated PPP over ATM on a Multipoint Subinterface

Multiple PVCs on multipoint subinterfaces significantly increase the maximum number of PPP-over-ATM sessions running on a Device.

Perform this task to configure IETF-compliant LLC encapsulated PPP over ATM PVC or a range of PVCs on a multipoint subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number.subinterface-number* **multipoint**
4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   -
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **encapsulation aal5mux ppp virtual-template** *number*
6. **protocol ppp virtual-template** *number*
7. Do one of the following:
   - **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 atm** *number.subinterface-number* **multipoint** **Example:** `Device(config)# interface atm 1/0/0.4 multipoint`	Specifies the ATM multipoint subinterface using the appropriate form of the **interface atm**command[10] and enters subinterface configuration mode.
Step 4	Do one of the following: • **pvc** [*name*] *vpi* / *vci* • • **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Device(config-subif)# pvc cisco 0/5` **Example:**	Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.

	Command or Action	Purpose
	or **Example:** `Device(config-subif)# range range1 pvc 1/200 1/299`	

Step 5	**encapsulation aal5mux ppp virtual-template** *number*
	Example:
	`Device(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3`
	Example:
	or
	Example:
	`Device(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3`
		Configures VC multiplexed encapsulation on a PVC or PVC range.

Step 6	**protocol ppp virtual-template** *number*
	Example:
	`Device(config-subif-atm-vc)# protocol ppp virtual-template 2`
	Example:
	or
	Example:
	`Device(config-subif-atm-range)# protocol ppp virtual-template 2`
		Configures IETF PPP over ATM LLC encapsulation on the PVC or a range of PVCs.

Step 7	Do one of the following:
	• **end**
	Example:
	`Device(config-subif-atm-vc)# end`
	Example:
	Example:
	`Device(config-subif-atm-range)# end`
		Exits ATM virtual circuit subinterface configuration mode.
		or
		Exits ATM range subinterface configuration mode.

What to do next

You can also configure IETF-compliant LLC encapsulated PPP over ATM in a VC class and apply this VC class to an ATM VC, subinterface, or interface. For information about configuring a VC class, see the "Configuring VC Classes" section in the Configuring ATM module.

Configuration Examples for PPP over ATM

IETF-Compliant MUX Encapsulated PPP over ATM Configuration

This section provides the following examples for configuring IETF-compliant PPP over ATM:

Example: ETF-Compliant PPP over ATM with Different Traffic-Shaping Parameters

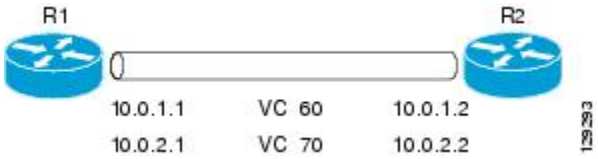
PVCs with different PPP-over-ATM traffic-shaping parameters can be configured on the same subinterface. In the following example, three PVCs are configured for PPP over ATM on subinterface ATM 2/0.1. PVC 0/60 is configured with IETF-compliant PPP over ATM encapsulation. Its traffic-shaping parameter is an unspecified bit rate with peak cell rate at 500 kb/s. PVC 0/70 is also configured with IETF-compliant PPP over ATM encapsulation, but its traffic-shaping parameter is nonreal-time variable bit rate, with peak cell rate at 1 Mb/s, sustainable cell rate at 500 kb/s, and burst cell size of 64 cells.

```
interface atm 2/0.1 multipoint
 pvc 0/60
  encapsulation aal5mux ppp virtual-template 3
   ubr 500
  exit
pvc 0/70
 encapsulation aal5mux ppp virtual-template 3
 vbr-nrt 1000 500 64
  exit
```

Example: Two Routers with Back-to-Back PVCs

The figure below illustrates an ATM interface with two PPP sessions over two PVC session connections. The sample commands following the figure establish the back-to-back router configuration.

Figure 12: Two Routers with Back-to-Back PVCs



R1 Configuration

```
interface atm 2/0
atm clock internal
pvc 0/60
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
pvc 0/70
```

```
encapsulation aal5mux ppp virtual-template 2
vbr-nrt 90 50 1024
exit
interface virtual-template 1
ip address 10.0.1.1 255.255.255.0
interface virtual-template 2
ip address 10.0.2.1 255.255.255.0
exit
```

R2 Configuration

```
interface atm 2/0.1 multipoint
pvc 0/60
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
pvc 0/70
encapsulation aal5mux ppp virtual-template 2
vbr-nrt 90 50 1024
exit
exit
interface virtual-template 1
ip address 10.0.1.2 255.255.255.0
exit
interface virtual-template 2
ip address 10.0.2.2 255.255.255.0
```

Example: Multiplexed Encapsulation Using VC Class

In the following example, PVC 0/60 is configured on subinterface ATM 2/0.1 with a VC class attached to it. By rule of inheritance, PVC 0/60 runs with IETF-compliant PPP over ATM encapsulation using the configuration from interface virtual-template 1. Its parameter is an unspecified bit rate with peak cell at 90 kb/s.

```
interface atm 2/0/0.1
pvc 0/60
class-vc pvc-ppp
exit
exit
vc-class atm pvc-ppp
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
```

IETF-Compliant LLC Encapsulated PPP over ATM Configuration

This section provides the following examples for configuring IETF-compliant LLC encapsulated PPP over ATM:

Example: Configuring IETF-Compliant PPP over ATM LLC Encapsulation

This example shows how to configure IETF PPP over ATM LLC encapsulation in the VC class called ppp-default. The VC class specifies virtual template 1 from which to spawn PPP interfaces, SNAP encapsulation (the default), and a UBR class traffic type at 256 kb/s. When the VC class ppp-default is configured on interface 0.1, PVC 0/70 inherits these properties. PVC 0/80 overrides virtual template 1 in the VC class and uses virtual template 2 instead. PVC 0/90 also overrides virtual template 1 and uses virtual template 3 instead. In addition, PVC 0/90 uses a VC multiplexed encapsulation and a UBR class traffic type at 500 kb/s.

```
interface atm 2/0/0.1 multipoint
class-int ppp-default
!
pvc 0/70
exit
!
pvc 0/80
protocol ppp virtual-template 2
exit
!
pvc 0/90
encapsulation aal5mux ppp virtual-template 3
ubr 500
exit
exit
!
vc-class atm ppp-default
protocol ppp virtual-template 1
ubr 256
exit
```

Example: Overriding a Virtual Template for IETF-Compliant PPP over ATM

This example illustrates how to use inheritance to override a virtual template configuration for muxppp encapsulation options. For PVC 5/505 the encapsulation option at that level is ciscoppp virtual template 1, as specified in the VC class called muxppp, the **protocol ppp virtual-template 2** command overrides only the virtual-template configuration.

```
interface atm 2/0/0.1
class-int muxppp
!
pvc 5/505
protocol ppp virtual-template 2
exit
!
muxppp
encapsulation aal5mux ppp virtual-template 1
exit
```

Example: Disabling IETF-Compliant PPP over ATM LLC Encapsulation on a Specific VC

This example shows how to limit the configuration of a particular LLC encapsulated protocol to a particular VC. First, we see that the VC class called ppp is configured with IETF PPP over ATM with LLC encapsulation and virtual template 1. This VC class is then applied to ATM interface 1/0/0. By configuring SNAP encapsulation by itself on PVC 0/32, you disable IETF PPP over ATM with LLC encapsulation on this particular PVC; PVC 0/32 will only carry IP.

```
interface atm 1/0/0
class-int ppp
exit
!
interface atm 1/0/0.100 point-to-point
description IP only VC
ip address 10.1.1.1 255.255.255.0
pvc 0/32
encapsulation aal5snap
exit
exit
!
```

```
vc-class atm ppp
encapsulation aal5snap
protocol ppp virtual-template 1
exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband and DSL commands	Cisco IOS Broadband and DSL Command Reference
Broadband access aggregation preparation tasks	Preparing for Broadband Access Aggregation
Configuring ATM	Configuring ATM

Standards/RFCs

Standards	Title
Frame Relay Forum standard FRF.8	*Frame Relay to ATM Internetworking*
RFC 2364	*PPP over AAL5*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

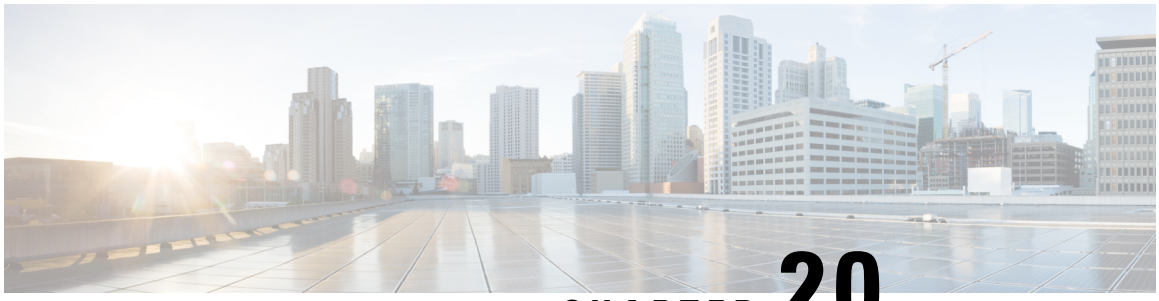
Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 20: Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Feature Name	Releases	Feature Configuration Information
PPP over ATM	Cisco IOS XE Release 3.3S Cisco IOS Release XE 3.14S	PPP over ATM provides support for the termination of multiple PPP connections on an ATM interface of a router. In Cisco IOS XE Release 3.3S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE Release 3.14S, support for this feature was added on the Cisco 4451-X Integrated Services Router. The following commands were introduced or modified: **encapsulation aal5mux ppp virtual-template** , **interface atm, protocol ppp virtual-template, pvc, range.**



CHAPTER 20

Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

The Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs feature provides the functionality of bridged ATM interface support to ATM switched virtual circuits (SVCs). Unlike permanent virtual circuits (PVCs), SVCs must be triggered by ongoing traffic and can be brought down when idle for some time. The SVCs are triggered, if down, and the traffic is passed on to the SVCs belonging to bridged ATM interface.

ATM routed bridge encapsulation (RBE) is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

Prerequisites for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

- When ATM SVCs are used, support for a form of bridging, such as integrated routing and bridging, is required.
- Before configuring connectivity from a remote bridged Ethernet network to a routed network using ATM routed bridge encapsulation, you must understand the concepts in the Understanding Broadband Access Aggregation module.

Restrictions for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

- Unlike PVCs, SVCs must be triggered by ongoing traffic and might be brought down after they have been idle for some time. The Bridged 1483 Encapsulated Traffic over ATM SVCs feature allows for the SVC to be triggered if down, and to pass the traffic on to the SVCs belonging to the bridged ATM interface.
- ATM RBE does not support MAC-layer access lists; only IP access lists are supported.

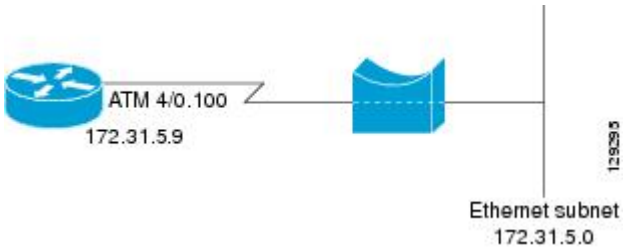
Information About Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

Overview on Bridged 1483 Encapsulated Traffic over ATM SVCs

ATM RBE is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

The figure below shows an ATM subinterface on a headend router that is configured to function in ATM routed-bridge encapsulation mode. This configuration is useful when a remote bridged Ethernet network device needs connectivity to a routed network via a device bridging from an Ethernet LAN to an ATM RFC 1483 bridged encapsulation.

Figure 13: ATM Routed Bridge Encapsulation



Because PVCs are statically configured along the entire path between the end systems, it would not be suitable to route bridged encapsulated traffic over them when the user wants to configure the virtual circuits (VCs) dynamically and tear down the VCs when there is no traffic.

ATM RBE Subinterface Grouping by PVC Range

You can configure ATM routed bridge encapsulation using an ATM PVC range rather than individual PVCs. When you configure a PVC range for routed bridge encapsulation, a point-to-point subinterface is created for each PVC in the range. The number of PVCs in a range can be calculated using the following formula:

number of PVCs = (end-vpi - start-vpi + 1) x (end-vci - start-vci +1)

Subinterface numbering begins with the subinterface on which the PVC range is configured and increases sequentially through the range.

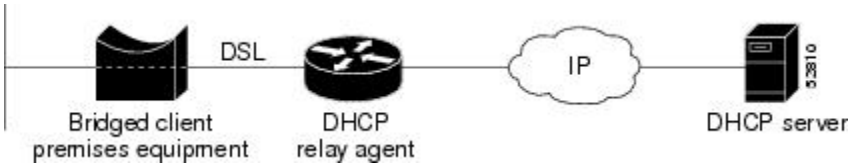
Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

DHCP Option 82 Support for RBE

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

The DHCP Option 82 Support for RBE feature provides support for the DHCP relay agent information option when ATM RBE is used. The figure below shows a typical network topology in which ATM RBE and DHCP are used. The aggregation router that is using ATM RBE is also serving as the DHCP relay agent.

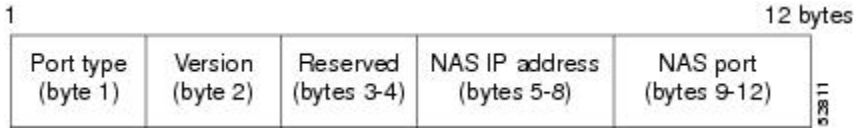
Figure 14: Network Topology Using ATM RBE and DHCP



This feature communicates information to the DHCP server using a suboption of the DHCP relay agent information option called *agent remote ID* . The information sent in the agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

The figure below shows the format of the agent remote ID suboption.

Figure 15: Format of the Agent Remote ID Suboption



The table below describes the agent remote ID suboption fields displayed in the figure above.

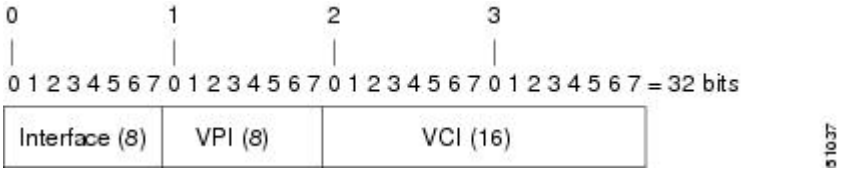
Table 21: Agent Remote ID Suboption Field Descriptions

Field	Description
Port Type	Port type. The value 0x01 indicates RBE. (1 byte)
Version	Option 82 version. The value 0x01 specifies the RBE version of Option 82 (1 byte).
Reserved	RBE reserved (2 bytes).
NAS IP Address	One of the interfaces on the DHCP relay agent. The **rbe nasip** command can be used to specify which IP address will be used. (4 bytes)

Field	Description
NAS Port	RBE-enabled virtual circuit on which the DHCP request has come in. See the figure below for the format of this field. (4 bytes)

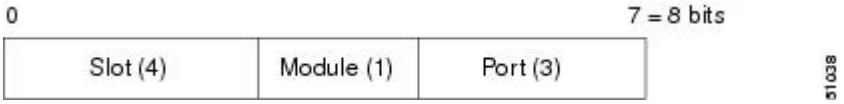
The figure below shows the format of the network access server (NAS) port field in the agent remote ID suboption.

Figure 16: Format of the NAS Port Field



The figure below shows the format of the interface field. If there is no module, the value of the module bit is 0.

Figure 17: Format of the Interface Field



DHCP Lease Limit per ATM RBE Unnumbered Interface

The DHCP lease limit per ATM RBE Unnumbered Interface feature is enabled on a Cisco IOS DHCP relay agent connected to clients through unnumbered interfaces. The relay agent keeps information about the DHCP leases offered to the clients per subinterface. When a DHCPACK message is forwarded to the client, the relay agent increments the number of leases offered to clients on that subinterface. If a new DHCP client tries to obtain an IP address and the number of leases has already reached the configured lease limit, DHCP messages from the client will be dropped and will not be forwarded to the DHCP server.

If this feature is enabled on the Cisco IOS DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

Benefits of Providing Connectivity Using ATM Routed Bridge Encapsulation

Bridged IP packets received on an ATM interface configured in routed-bridge mode are routed via the IP header. Such interfaces take advantage of the characteristics of a stub LAN topology commonly used for digital subscriber line (DSL) access and offer increased performance and flexibility over integrated routing and bridging (IRB).

Another benefit of ATM RBE is that it reduces the security risk associated with normal bridging or IRB by reducing the size of the nonsecured network. By using a single VC allocated to a subnet (which could be as small as a single IP address), ATM RBE uses an IP address in the subnet to limit the "trust environment" to the premises of a single customer.

ATM RBE supports Cisco Express Forwarding (CEF), fast switching, and process switching.

The DHCP Option 82 Support for RBE feature enables those service providers to use DHCP to assign IP addresses and DHCP option 82 to implement security and IP address assignment policies.

The DHCP Lease Limit per ATM RBE Unnumbered Interface feature allows an Internet service provider (ISP) to globally limit the number of leases available to clients per household or connection.

How to Configure ATM Routed Bridge Encapsulation over PVCs

Configuring ATM Routed Bridge Encapsulation Using PVCs

Perform the following task to configure ATM RBE using PVCs. Only the specified network layer (IP) is routed. Any remaining protocols can be passed on to bridging or other protocols. In this manner, ATM RBE can be used to route IP, while other protocols (such as IPX) are bridged normally.

or

show ip cache verbose

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / **0** . *subinterface-number* **point-to-point**
4. Do one of the following:
   - **pvc** *vpi* /*vci*
   -
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **exit**
6. **ip address** *ip-address mask* [**secondary**]
7. **end**
8. Do one of the following:
   - **show arp**
   - or
   - **show ip cache verbose**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**interface atm** *slot* **/ 0 .** *subinterface-number* **point-to-point** **Example:** `Router(config)# interface atm 5/0.5 point-to-point`	Specifies an ATM point-to-point subinterface and enters subinterface mode.

Step 4	Do one of the following:
	• **pvc** *vpi* /*vci*
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	Example:
	`Router(config-subif)# pvc 0/32`
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures a PVC to carry the routed bridge traffic and enters ATM VC class configuration mode.
		Configures a range of PVCs to carry the routed bridge traffic and enters ATM PVC range configuration mode.

Step 5	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits to subinterface configuration mode.
Step 6	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 209.165.200.224 255.255.255.0`	Provides an IP address on the same subnetwork as the remote network.
Step 7	**end** **Example:** `Router(config-subif)# end`	Exits to privileged EXEC mode.

Step 8	Do one of the following:
	• **show arp**
	• or
	• **show ip cache verbose**
	Example:
	`Router# show arp`
	Example:
	`Router# show ip cache verbose`
		(Optional) Displays ATM RBE configuration information.

Examples

To confirm that ATM RBE is enabled, use the **show arp** command and the **show ip cache verbose** command in privileged EXEC mode:

```
Router# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  209.165.201.51         6   0001.c9f2.a81d  ARPA   Ethernet3/1
Internet  209.165.201.49         -   0060.0939.bb55  ARPA   Ethernet3/1
Internet 209.165.202.128        30   0010.0ba6.2020  ARPA   Ethernet3/0
Internet 209.165.201.52          6   00e0.1e8d.3f90  ARPA   ATM1/0.4
Internet 209.165.201.53          5   0007.144f.5d20  ARPA   ATM1/0.2
Internet 209.165.202.129         -   0060.0939.bb54  ARPA   Ethernet3/0
Internet 209.165.201.125        30   00b0.c2e9.bc55  ARPA   Ethernet3/1#
Router# show ip cache verbose
IP routing cache 3 entries, 572 bytes
   9 adds, 6 invalidates, 0 refcounts
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 00:30:34 ago
Prefix/Length       Age       Interface  Next Hop
209.165.201.51/32-24 00:30:10  Ethernet3/1 10.1.0.51 14  0001C9F2A81D00600939 BB550800
209.165.202.129/32-24 00:00:04 ATM1/0.2  10.8.100.50 28
00010000AAAA030080C2000700000007144F5D2000600939 BB1C0800
209.165.201.125/32-24 00:06:09 ATM1/0.4  10.8.101.35 28
00020000AAAA030080C20007000000E01E8D3F9000600939 BB1C0800
```

Configuring DHCP Option 82 for RBE

Perform this task to configure the DHCP Option 82 Support for RBE feature.

Before you begin

DHCP option 82 support must be configured on the DHCP relay agent using the **ip dhcp relay information option** command before you can use the DHCP Option 82 Support for RBE feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **rbe nasip** *source-interface*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp relay information option** **Example:** `Router(config)# ip dhcp relay information option`	Enables the DHCP option 82 support on relay agent. • Enabling the DHCP option 82 support allows the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.
Step 4	**rbe nasip** *source-interface* **Example:** `Router(config)# rbe nasip loopback0`	Specifies the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the Agent Remote ID suboption.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged configuration mode.

Configuring the DHCP Lease Limit

Perform this task to limit the number of DHCP leases allowed on ATM RBE unnumbered or serial unnumbered interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease per interface** *lease-limit*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**ip dhcp limit lease per interface** *lease-limit* **Example:** `Router(config)# ip dhcp limit lease per interface 2`	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting the DHCP Lease Limit

Perform this task to troubleshoot the DHCP lease limit.

SUMMARY STEPS

1. **enable**
2. **debug ip dhcp server packet**
3. **debug ip dhcp server events**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip dhcp server packet** **Example:** `Router# debug ip dhcp server packet`	(Optional) Decodes DHCP receptions and transmissions.
Step 3	**debug ip dhcp server events** **Example:** `Router(config)# debug ip dhcp server events`	(Optional) Displays server events.

Configuration Examples for Providing Connectivity Using ATM Routed Bridge Encapsulation

The following examples show various ways to provide connectivity from a remote bridged network to a routed network using ATM RBE.

Example Configuring ATM RBE on PVCs

The following example shows a typical ATM routed bridge encapsulation configuration:

```
enable
 configure terminal
 interface atm 4/0.100 point-to-point
  ip address 209.165.200.225 255.255.255.224
   pvc 0/32
    end
```

Example Configuring ATM RBE on an Unnumbered Interface

The following example uses a static route to point to an unnumbered interface:

```
 enable
  configure terminal
  interface loopback 0
  ip address 209.165.200.226 255.255.255.224
  interface atm 4/0.100 point-to-point
   ip unnumbered loopback 0
   pvc 0/32
    atm route-bridge ip
    exit
  ip route 209.165.200.228 255.255.255.224 atm 4/0.100
  end
```

Example Concurrent Bridging and ATM RBE

The following example shows concurrent use of ATM RBE with normal bridging. IP datagrams are route-bridged, and other protocols (such as IPX or AppleTalk) are bridged.

```
bridge 1 protocol ieee
interface atm 4/0.100 point-to-point
 ip address 209.165.200.225 255.255.255.224
 pvc 0/32
 bridge-group 1
 atm route-bridge ip
```

Example DHCP Option 82 for RBE Configuration

In the following example, DHCP option 82 support is enabled on the DHCP relay agent using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server.

```
ip dhcp-server 209.165.200.225
!
ip dhcp relay information option
!
interface Loopback0
 ip address 209.165.201.0 255.255.255.248
!
interface atm 4/0
 no ip address
!
interface atm 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 209.165.201.3
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
!
interface Ethernet5/1
 ip address 209.165.201.4 255.255.255.248
!
router eigrp 100
 network 209.165.201.0
 network 209.165.200.0
!
rbe nasip Loopback0
```

For the configuration example, the value (in hexadecimal) of the agent remote ID suboption would be 010100000B01018140580320. The table below shows the value of each field within the agent remote ID suboption.

Table 22: Agent Remote ID Suboption Field Values

Agent Remote ID Suboption Field	Value
Port Type	0x01
Version	0x01
Reserved	undefined
NAS IP Address	0x0B010181 (hexadecimal value of 11.1.1.129)
NAS Port • Interface (slot/module/port) • VPI • VCI	• 0x40 (The slot/module/port values are 01 00/0/000.) • 0x58 (hexadecimal value of 88) • 0x320 (hexadecimal value of 800)

Example DHCP Lease Limit

In the following example, if more than three clients try to obtain an IP address from interface ATM4/0.1, the DHCPDISCOVER packets will not be forwarded to the DHCP server. If the DHCP server resides on the same router, DHCP will not reply to more than three clients.

```
ip dhcp limit lease per interface 3
!
interface loopback0
 ip address 209.165.201.3 255.255.255.248
!
interface atm 4/0.1
 no ip address
!
interface atm 4/0.1 point-to-point
 ip helper-address 172.16.1.2
 ip unnumbered loopback0
 atm route-bridged ip
  pvc 88/800
  encapsulation aal5snap
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband Access Aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Preparing for broadband access aggregation task	Preparing for Broadband Access Aggregation
DHCP commands	*Cisco IOS IP Addressing Services Command Reference*
DHCP configuration tasks	"Configuring the Cisco IOS DHCP Server" module in the *Cisco IOS IP Addressing Services Configuration Guide*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation

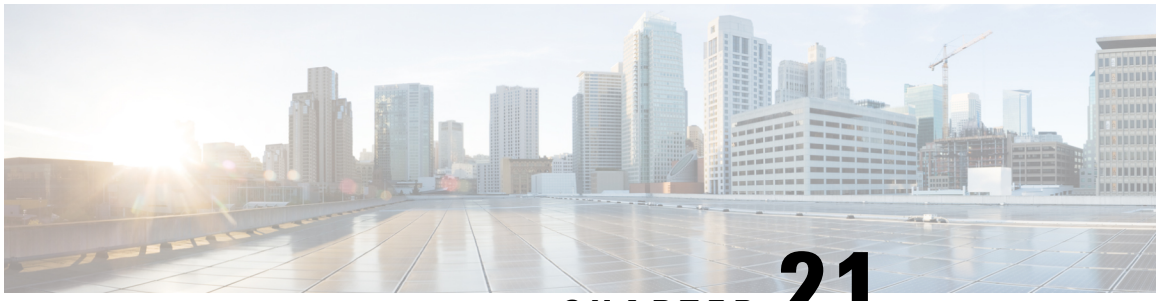
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 23: Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation

Feature Name	Releases	Feature Information
Bridged 1483 Encapsulated Traffic over ATM SVCs	12.4(15)T 12.2(33)SRE	The Bridged 1483 Encapsulated Traffic over ATM SVCs feature provides support for bridged 1483 encapsulated packets to trigger ATM SVC and also support for sending this traffic on triggered ATM SVCs.
DHCP Option 82 Support for Routed Bridge Encapsulation	15.1(1)S 12.2(2)T	This feature provides support for the DHCP relay agent information option when ATM RBE is used. The following command was introduced:**rbe nasip**

Feature Name	Releases	Feature Information
DHCP Lease Limit per ATM RBE Unnumbered Interface	12.3(2)T	This feature limits the number of DHCP leases per subinterface offered to DHCP clients connected from an ATM RBE unnumbered interface or serial unnumbered interface of the DHCP server or DHCP relay agent. The following command was introduced:**ip dhcp limit lease per interface**



CHAPTER 21

PPPoE Circuit-Id Tag Processing

The PPPoE Circuit-Id Tag Processing feature provides a way to extract a Circuit-Id tag from the digital subscriber line (DSL) as an identifier for the authentication, authorization, and accounting (AAA) access request on a Fast Ethernet or Gigabit Ethernet interface, thereby simulating ATM-based Broadband access, but using cost-effective Fast Ethernet or Gigabit Ethernet instead. The tag is useful for troubleshooting the network, and is also used in RADIUS authentication and accounting processes.

Prerequisites for the PPPoE Circuit-Id Tag Processing Feature

It is recommended that you be familiar with RFC 2516 before configuring this feature.

Information About the PPPoE Circuit-Id Tag Processing Feature

Differences Between ATM- and Fast or Gigabit Ethernet-Based Broadband Access Networks

Broadband digital subscriber line multiplexer (DSLAM) and Broadband Remote Access Server (BRAS) vendors see a need to provide Fast or Gigabit Ethernet-based networks as an alternative to an ATM access network, with a DSLAM bridging the ATM-DSL local loop to the Fast or Gigabit Ethernet-based access network and allowing Fast or Gigabit Ethernet-based connectivity to the BRAS. But in an Fast or Gigabit Ethernet access network, there is no unique mapping between the subscriber Line-Id and the interface, as is found in an ATM-based network. In an ATM-based network, the ATM VC is associated to a subscriber line.

During the authentication phase that initiates the PPP access and AAA accounting requests, the BRAS includes a NAS-Port-Id attribute in RADIUS authentication packets, if the feature "TAL based on the NAS-Port-Id" feature is configured. This attribute identifies the DSL line for the subscriber. See Configuring BRAS to Include a NAS-Port-Id Attribute Example, on page 243 for an example.

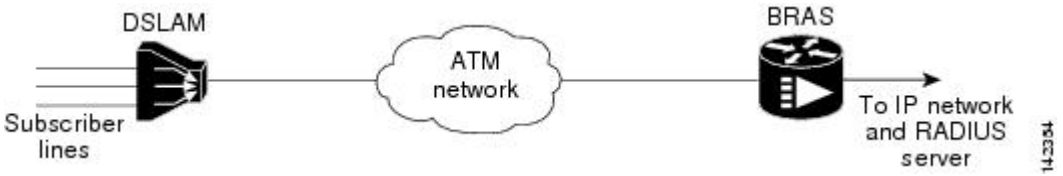
DSL Forum 2004-71 Solution

To apply the same subscriber mapping capability to Fast or Gigabit Ethernet interfaces that is possible on ATM interfaces, DSL Forum 2004-71 proposes a solution whereby the DSLAM sends the DSL Line-Id in the PPP over Ethernet (PPPoE) discovery phase. This method provides a way for a PPPoE server acting as a BRAS to extract the Line-Id tag and use the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests. The PPPoE Circuit-Id Tag Processing feature makes use of the proposed DSL Forum 2004-71 method and allows the BRAS to detect the presence of the subscriber Circuit-Id tag inserted by the DSLAM during the PPPoE discovery phase. The BRAS will send this tag as a NAS-Port-Id attribute in PPP authentication and AAA accounting requests. The tag is useful in troubleshooting the Ethernet network, and it is also used in RADIUS authentication and accounting processes.

Approach for a Circuit-Id Tag in Ethernet-Based Broadband Access Networks

Traditional ATM-based DSL broadband access networks have the topology shown in the figure below.

Figure 18: ATM-Based DSL Broadband Access Network

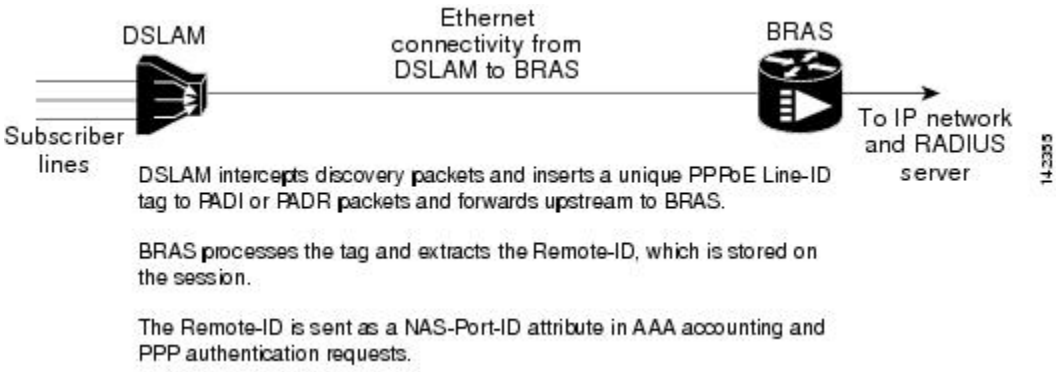


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM VC used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-Id for use in RADIUS packets.

The simple mapping available from an ATM-based network between the physical line in the DSL local loop to the end user and a VC (from DSLAM to BRAS) is not available for an Fast or Gigabit Ethernet-based network. To solve this problem, the PPPoE Circuit-Id Tag Processing feature uses a PPPoE intermediate agent function on the DSLAM to attach a tag to the PPPoE discovery packets. The BRAS then receives the tagged packet, decodes the tag, and inserts the line identifier into RADIUS packets destined for the RADIUS server.

DSLAM intercepts PPPoE discovery frames from the client and inserts a unique line identifier (circuit-id) using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation and Request (PADI and PADR) packets; see the figure below. The DSLAM forwards these packets to the BRAS after the insertion. The tag contains the circuit-id of the DSL line on which the PADI or PADR packet was received, in the access node where the intermediate agent resides.

Figure 19: PPPoE Circuit-Id Tag Processing Solution



When the **vendor-tag circuit-id service** command is configured in BBA (broadband access) group configuration mode, the BRAS processes the received PPPoE Vendor-Specific tag in the PADR packet and extracts the Circuit-Id field, which is sent to the remote AAA server as the NAS-Port-Id attribute (RADIUS attribute 87) in RADIUS access and accounting requests. When the **radius-server attribute nas-port format d** global configuration command is also configured on the BRAS, the Acct-Session-Id attribute will contain the information about the incoming access interface, where discovery frames are received, and about the session being established.

Outgoing PAD Offer and Session-confirmation (PADO and PADS) packets from the BRAS will have the DSLAM-inserted Circuit-Id tag. DSLAM should strip the tag out of PADO and PADS packets. If the DSLAM cannot strip off the tag, the BRAS should remove it before sending the packets out, and this is accomplished using the **vendor-tag circuit-id strip** BBA group configuration mode command.

Benefits of the PPPoE Circuit-Id Tag Processing Feature

The shift towards Fast or Gigabit Ethernet-based DSLAMs offers the following benefits:

- Ability to use simpler and lower cost provisioning options for DSL subscribers over an Fast or Gigabit Ethernet-based backhaul network rather than on an ATM-based network.
- Ability to use higher bandwidth connectivity options available from Fast or Gigabit Ethernet not possible on ATM.
- Ability to upgrade to next-generation DSLAMs with quality of service (QoS), and support for higher bandwidth, asymmetric dual latency modems such as the ADSL2.
- Ability to inject high-bandwidth content such as video in an Ethernet network.

How to Configure the PPPoE Circuit-Id Tag Processing Feature

Configuring the PPPoE Circuit-Id Tag Processing Feature

This section describes how to configure an Fast or Gigabit Ethernet-based access network on a Cisco BRAS. The extracted Circuit-Id tag (see Information About the PPPoE Circuit-Id Tag Processing Feature, on page 237) is sent in the following RADIUS syntax, as recommended by the DSL Forum:

"Access-Node-Identifier eth *slot/port* [**:***vlan-tag*]"

The Access-Node-Identifier is a unique subscriber identifier or telephone number text string entered without spaces. Per DSL-Forum 2004-71, the maximum length supported for the tag is 48 bytes. The BRAS copies the entire tag into the NAS-Port-Id and sends it to the AAA server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **bba-group pppoe** *group-name*
5. **vendor-tag circuit-id service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute nas-port format d** **Example:** `Router(config)# radius-server attribute nas-port format d`	(Optional) Selects the PPPoE extended NAS-Port format used for RADIUS access and accounting. • Configure this command so that the Acct-Session-Id attribute, as displayed in the **debug radius** command, will contain the information about the incoming access interface, where discovery frames are received, and about the session being established. See the Displaying the Session Activity Log, on page 241 and Configuration Examples for the PPPoE Circuit-Id Tag Processing Feature, on page 243 sections for more information.
Step 4	**bba-group pppoe** *group-name* **Example:** `Router(config-bba-group)# bba-group pppoe pppoe-group`	Defines a PPPoE profile.
Step 5	**vendor-tag circuit-id service** **Example:**	Enables processing of the received PPPoE Vendor-Specific tag in the PADR packet, which extracts the Circuit-Id part of the tag and sends it to the AAA server as the NAS-Port-Id attribute in RADIUS access and accounting requests.

	Command or Action	Purpose
	`Router(config-bba-group)# vendor-tag circuit-id service`	

Removing the PPPoE Circuit-Id Tag

Outgoing PADO and PADS packets will have the DSLAM-inserted Vendor-Specific Line-Id tag, and DSLAM must strip the Circuit-Id tag from the packets. If the DSLAM cannot strip the tag, the BRAS must remove it before sending out the packets. This task is accomplished through configuration of the **vendor-tag circuit-id strip** command in BBA group configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**vendor-tag strip** **Example:** `Router(config-bba-group)# vendor-tag strip`	Enables the BRAS to strip off incoming Vendor-Specific Circuit-Id tags from outgoing PADO and PADS packets.

Displaying the Session Activity Log

When the **radius-server attribute nas-port format d** global configuration command is added to the PPPoE Circuit-Id Tag Processing feature configuration on the BRAS (see the Configuring PPPoE Circuit-Id Tag Processing Example, on page 243 for an example), the report from the **debug radius** privileged EXEC command

will include information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

Enable the **debug radius** command to display a report of session activity. In the example shown in this section:

- The acct_session_id is 79 or 4F in hexadecimal format.
- In the message "Acct-session-id pre-pended with Nas Port = 0/0/0/200," the interface on which the PPPoE discovery frames arrived is FastEthernet0/0.200. The 0/0/0 is Cisco format for slot/subslot/port.
- The Acct-Session-Id vendor-specific attribute 44 contains the string "0/0/0/200_0000004F," which is a combination of the ingress interface and the session identifier.

Note Strings of interest in the **debug radius** output log are presented in bold text for example purposes only.

```
Router# debug radius
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Access-Request to 172.20.164.143:1645 id 1645/65, len 98
02:10:49: RADIUS:  authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32
02:10:49: RADIUS:  authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                     [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION    Event PPP_LOCAL
02:10:49: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server 172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1 646/42, len
 117
02:10:49: RADIUS:  authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
02:10:49: RADIUS:  Acct-Session-Id     [44]  20  "0/0/0/200_0000004F"
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                        [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic      [45]  6 RADIUS                     [1]
02:10:49: RADIUS:  Acct-Status-Type    [40]  6 Start                      [1]
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                   [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
```

```
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                   [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time     [41]  6   0
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len
20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

Configuration Examples for the PPPoE Circuit-Id Tag Processing Feature

Configuring PPPoE Circuit-Id Tag Processing Example

In the following example, outgoing PADO and PADS packets will retain the incoming Vendor-Specific Circuit-Id tag:

```
radius-server attribute nas-port format d
!
bba-group pppoe pppoe-group
 sessions per-mac limit 50
 vendor-tag circuit-id service
!
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

Configuring BRAS to Include a NAS-Port-Id Attribute Example

In the following example, the feature TAL based on the NAS-Port-Id is configured. This configuration ensures that a NAS-Port-Id attribute is included in RADIUS authentication packets during the authentication phase to initiate PPP access and AAA accounting requests.

```
radius-server attribute nas-port
policy-map type control test
 class type control always event session-start
 1 authorize identifier nas-port
```

Removing the PPPoE Circuit-Id Tag Example

In the following example, the BRAS will strip off incoming Vendor-Specific Circuit-Id tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service
 vendor-tag strip
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

Additional References

The following sections provide references related to the PPPoE Circuit-Id Tag Processing feature.

Related Documents

Related Topic	Document Title
Configuring Broadband and DSL	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
RADIUS attributes	*Cisco IOS XE Security Configuration Guide*
DSL Forum Line-Id tag solution	Broadband Forum

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

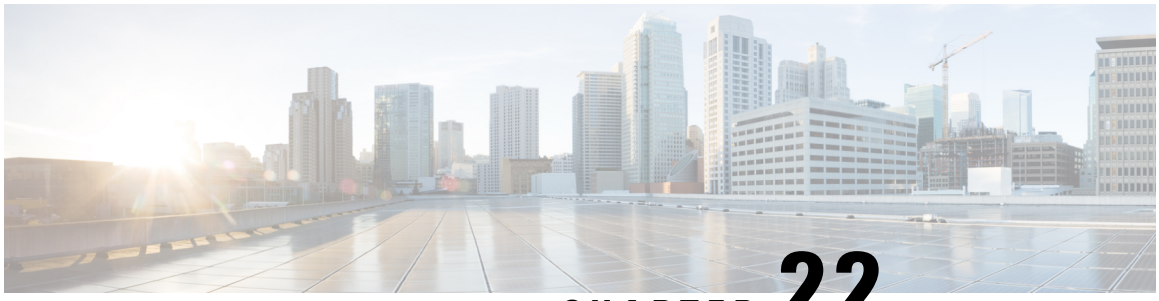
Feature Information for PPPoE Circuit-Id Tag Processing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 24: Feature Information for PPPoE Circuit-Id Tag Processing

Feature Name	Releases	Feature Information
PPPoE Circuit-Id Tag Processing	Cisco IOS XE Release 2.1.	The PPPoE Circuit-Id Tag Processing feature provides a way to extract a Circuit-Id tag from the DSL as an identifier for the AAA access request on an Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Ethernet instead. The tag is useful for troubleshooting the network, and is also used in RADIUS authentication and accounting processes. This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature was integrated into Cisco IOS XE Release 2.3.1. The following commands were introduced or modified: **vendor-tag circuit-id service**, **vendor-tag strip**.



CHAPTER 22

Configuring PPP over Ethernet Session Limit Support

This module provides information on how to limit the number of PPP over Ethernet (PPPoE) sessions that can be created on a router or on a Gigabit Ethernet interface for configuration.

Information About Configuring PPP over Ethernet Session Limit Support

Benefits of Configuring PPP over Ethernet Session Limit Support

- The PPPoE Session Limit Support feature prevents the router from using too much memory for virtual access by limiting the number of PPPoE sessions that can be created on a router or on all Ethernet interfaces and subinterfaces as well as ATM interfaces and subinterfaces.
- The SNMP Enhancements for ASR 1000 feature enhances Cisco ASR 1000 Aggregation Series Router to count the PPPoE sessions in PTA, FWDED, and TRANS state for a particular physical interface, and the total number of sessions that exist in a physical interface. Provision for using a system-wide threshold trap and per-physical threshold trap is provided through SNMP. These functionalities enable users to retrieve the total number of sessions and per-interface session-loss threshold value.

Trap Generation

In scenarios where you must deploy ASR 1000 Series Routers with one physical port mapped to one DSLAM and if the total number of sessions for the DSLAM falls below the threshold value on a physical interface, due to a loss of high number of sessions, a notification trap is generated. You can use these traps to investigate the issue and take immediate actions.

When the number of active sessions falls below the threshold value, only one trap is generated. Further traps are not sent even if the number of sessions continue to decrease. The next set of traps are sent only if the number of sessions rise above the configured threshold value and fall. This criterion is applicable to both global and per-interface traps.

When threshold values are configured in both global and per-interface configuration modes, then both the threshold values are monitored separately. Traps are sent when the session count falls below the threshold value either in global configuration mode or in per-interface configuration mode.

How to Configure PPP over Ethernet Session Limit Support

Specifying the Maximum Number of PPPoE Sessions on a Router

Perform this task to specify the maximum number of PPPoE sessions that can be created on a router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id*]
7. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
8. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Configures a broadband aggregation (BBA) group to be used to establish PPPoE sessions and enters BBA group configuration mode. • *name* --Name of the BBA group. You can have multiple BBA groups.

	Command or Action	Purpose
		• **global** -- Specifies the PPPoE profile that serves as the default profile for any PPPoE port (Gigabit Ethernet interface or VLAN) that has not been assigned a specific PPPoE profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template that will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 1000`	(Optional) Configures the maximum number of PPPoE sessions allowed per MAC session limit in a PPPoE profile. The default MAC session limit is 100.
Step 6	**sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id*] **Example:** `Router(config-bba-group)# session per-vlan limit 4000 inner 3500`	(Optional) Sets the session limit for the inner VLAN on QinQ subinterface. The default session limit is 100. **Note** The per-VLAN limit is only applicable to Gigabit Ethernet subinterfaces (802.1q VLANs).
Step 7	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit 2000`	(Optional) Sets the maximum number of PPPoE sessions allowed per VC session limit in a PPPoE profile. The default session limit is 100. **Note** The per-VC limit is applicable only to ATM interfaces and subinterfaces.
Step 8	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 32000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated. **Note** This command applies only to the global profile.
Step 9	**exit** **Example:** `Router(config-bba-group)# exit`	Returns to global configuration mode.

Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface

Perform this task to specify the maximum number of PPPoE sessions that can be created on a Gigabit Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet** | **tenGigabitEthernet**} *slot* / *subslot* / *port*[**.** *subinterface*]
4. **pppoe enable** [**group** *group-name*]
5. **pppoe max-sessions** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**GigabitEthernet** | **tenGigabitEthernet**} *slot* / *subslot* / *port*[**.** *subinterface*] **Example:** `Router(config)# interface GigabitEthernet0/0/1`	Specifies a Gigabit Ethernet interface and enters interface configuration mode.
Step 4	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-if)# pppoe enable group one`	Enables PPPoE sessions on a Gigabit Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface through the use of the **group** *group-name* option, the interface will use the global PPPoE profile.
Step 5	**pppoe max-sessions** *number* **Example:** `Router(config-if)# pppoe max-sessions 10`	Specifies the maximum number of PPPoE sessions permitted on the interface or subinterface.
Step 6	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuring System-Wide Threshold Parameters

Performthis task to configure the system-wide threshold parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group ppp oe globa** l
4. **sessions threshold** *number*
5. **exit**
6. **interface** type *number*
7. **pppoe-sessions threshold** *number*
8. **end**
9. **show pppoe summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router> configure terminal`	Enters global configuration mode.
Step 3	**bba-group ppp oe globa** l **Example:** `Router(config)# bba-group pppoe global`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**sessions threshold** *number* **Example:** `Router(config-bba-group)# sessions threshold 1000`	Configures the global threshold value.
Step 5	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode and returns to privileged EXEC mode.
Step 6	**interface** type *number* **Example:** `Router(config-if)# interface GigabitEthernet 0/0`	Enters interface configuration mode.
Step 7	**pppoe-sessions threshold** *number* **Example:**	Configures per-session threshold value.

	Command or Action	Purpose
	`Router(config-if)# pppoe-sessions threshold 1000`	
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode
Step 9	**show pppoe summary** **Example:** `Router# show pppoe summary`	Displays the count of PPPoE sessions in PTA, FWDED, and TRANS state for a particular physical interface.

Configuration Examples for PPP over Ethernet Session Limit Support

Example Specifying the Maximum Number of PPPoE Sessions on a Router

The following example shows how to configure a limit of 1,000 PPPoE sessions for the router:

```
bba-group pppoe global
  virtual-template 1
  sessions per-mac limit 1000
  sessions per-vlan limit 4000 inner 3500
  sessions per-vc limit 2000
```

Example Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface

The following example shows how to configure a limit of ten PPPoE sessions on the Gigabit Ethernet interface:

```
interface GigabitEthernet 1/0/0
  pppoe enable
  pppoe max-sessions 10
```

The following example shows how to configure a limit of ten PPPoE sessions on the Gigabit Ethernet subinterface by using the **encapsulation**command:

```
interface GigabitEthernet 0/0/0.1
  encapsulation dot1q 2
  pppoe enable
  pppoe max-sessions 10
```

Example Configuring the System-wide Threshold Parameters

The following example shows how to configure global and per-session threshold values:

```
Router# configure terminal
Router(config)# bba-group pppoe global
 Router(config-bba-group)# sessions threshold 1000
Router(config-bba-group)# exit
Router# configure terminal

Router(config)# interface GigabitEthernet 0/0

Router(config-if)# pppoe-sessions threshold 90
Router(config-if)# end
```

The following example shows how to use the **show pppoe summary** command to display the count of the PPPoE sessions:

```
Router# show pppoe summary
PTA  : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA   FWDED TRANS
TOTAL 1       1       0       0
GigabitEthernet0/3/1 1       1       0       0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband and DSL commands	*Cisco IOS Broadband and DSL Command Reference*
Broadband access aggregation of PPPoE sessions	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring PPP over Ethernet Session Limit Support

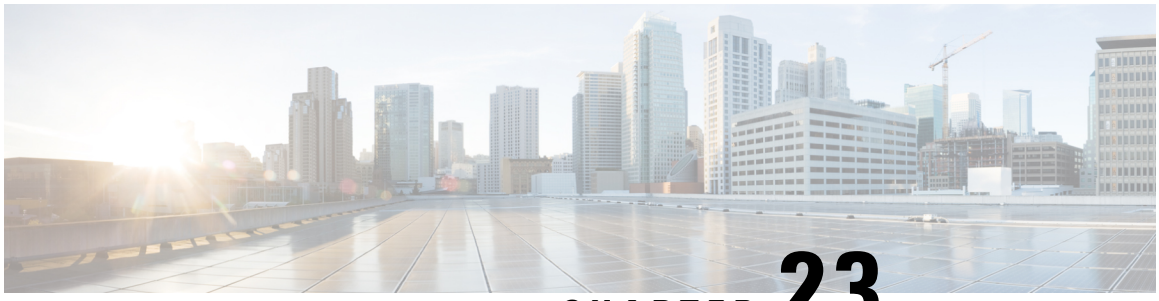
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 25: Feature Information for Providing PPP over Ethernet Session Limit Support

Feature Name	Releases	Feature Information
PPP over Ethernet Session Limit Support	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.4	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The PPPoE Session Limit Support feature enables you to limit the number of PPPoE sessions that can be created on a router or on a Gigabit Ethernet interface for configuration. This feature was integrated into Cisco IOS XE Release 2.4.

Feature Name	Releases	Feature Information
SNMP Enhancements for ASR 1000	Cisco IOS XE Release 3.2S	The SNMP Enhancements for ASR 1000 feature enhances Cisco ASR 1000 Aggregation Series Routers to provide the count of the PPPOE sessions in PTA, Forwarded, and TRANS state for a particular physical interface, and the total count of sessions that exist in a physical interface. This feature was introduced in Cisco IOS XE 3.2S. The following commands were introduced or modified: **pppoe-sessions threshold**, **sessions threshold**.



CHAPTER 23

PPPoE Session Limit Local Override

The PPPoE Session Limit Local Override feature enables the session limit configured locally on the broadband remote access server (BRAS) or L2TP access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is enabled.

Information About PPPoE Session Limit Local Override

How PPPoE Session Limit Local Override Works

PPP over Ethernet (PPPoE) session limits are downloaded from the RADIUS server when you enable SSS preauthorization on the LAC using the **subscriber access pppoe pre-authorize nas-port-id**command. By enabling preauthorization, you limit the number of PPPoE sessions on a specific VLAN; that is, the PPPoE per-NAS-port session limit downloaded from the RADIUS server takes precedence over locally configured (port-based) session limits, such as per-VLAN session limits. The following is a sample user profile to configure a session limit through RADIUS:

```
Username=nas_port:10.10.10.10:4/0/0/1.100
Password = "password1"
cisco-avpair= "pppoe:session-limit=session limit per NAS-port"
```

The PPPoE Session Limit Local Override feature enables the local session limit configured at the BRAS to override the per-NAS-port session limit configured at the RADIUS server when SSS preauthorization is configured.

Note The PPPoE Session Limit Local Override feature is useful only when you have configured SSS preauthorization on the BRAS or LAC.

To enable the PPPoE Session Limit Local Override feature, configure the **sessions pre-auth limit ignore** command under the broadband access (BBA) group associated with the interface. When the PPPoE Session

Limit Local Override feature is enabled, the locally configured session limit is applied before PPP is started; that is before the BRAS sends out a PPPoE Active Discovery Offer (PADO) packet to the client, advertising a list of available services.

When preauthorization is configured without the PPPoE Session Limit Local Override feature enabled, the client receives an authentication failure response from the BRAS when there is no session limit downloaded from the RADIUS server and the locally configured session limit is exceeded. The BRAS waits to apply locally configured limits until PPP negotiation is completed. When a call is finally rejected, the client receives the authentication failure response, resulting in session failure, with no ability to distinguish whether the session failure results from a Challenge Handshake Authentication Protocol (CHAP) authentication failure or a PPPoE session limit having been exceeded. The PPPoE Session Limit Local Override feature allows for differentiation between the handling of per-NAS-port failures and session limiting failures.

If you enable the PPPoE Session Limit Local Override feature, but there are no locally configured per-port session limits, then per-NAS-port session limits downloaded from the RADIUS server are applied.

How to Configure PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override

Enable the PPPoE Session Limit Local Override feature to allow the local session limit configured on the BRAS to override the per-NAS-port session limit downloaded from the RADIUS server.

Note If there are no locally configured per-port session limits, then per-NAS port session limits downloaded from the RADIUS server are applied.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **sessions per-vlan limit** *per-vlan-limit*
5. **sessions pre-auth limit ignore**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe test`	Creates a PPPoE profile and enters BBA group configuration mode. • *group-name* --Name of the PPPoE profile.
Step 4	**sessions per-vlan limit** *per-vlan-limit* **Example:** `Router(config-bba-group)# sessions per-vlan limit 3`	Limits the number of PPPoE sessions per VLAN in a PPPoE profile. • *per-vlan-limit* --Maximum number of PPPoE sessions that can be established over an Ethernet VLAN. The default is 100.
Step 5	**sessions pre-auth limit ignore** **Example:** `Router(config-bba-group)# sessions pre-auth limit ignore`	Enables the PPPoE Session Limit Local Override feature. The locally configured limit overrides the per-NAS-port session limit configured at the RADIUS server.
Step 6	**end** **Example:** `Router(config-bba-group)# end`	Exits BBA group configuration mode and returns to privileged EXEC mode.

Configuration Examples for PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override Example

The following example creates a PPPoE group named test, configures a limit of three sessions per VLAN, and enables the PPPoE Session Limit Local Override feature in bba-group configuration mode. The running configuration shows that the **sessions pre-auth limit ignore** command was used to enable this feature.

```
Router(config)# bba-group pppoe test
Router(config-bba-group)# sessions per-vlan limit 3
Router(config-bba-group)# sessions pre-auth limit ignore

.
.
!
bba-group pppoe test
virtual-template 2
sessions per-vlan limit 3
sessions pre-auth limit ignore
!
```

Additional References

The following sections provide references related to the PPPoE Session Limit Local Override feature.

Related Documents

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* •

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

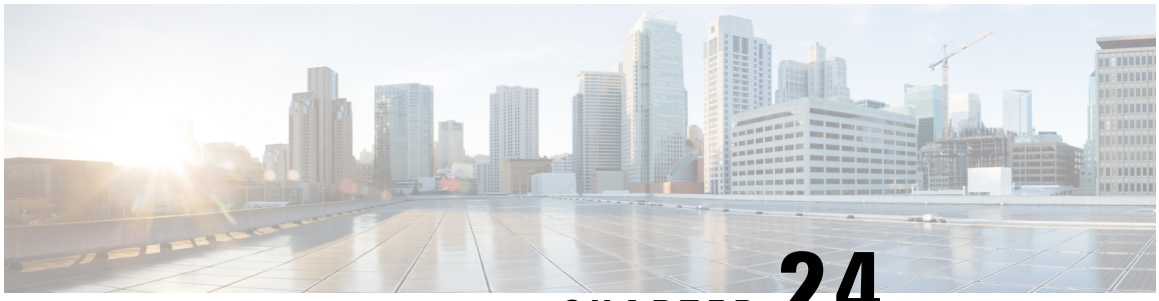
Feature Information for PPPoE Session Limit Local Override

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 26: Feature Information for PPPoE Session Limit Local Override

Feature Name	Releases	Feature Information
PPPoE--Session Limit Local Override	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. This feature enables the session limit configured locally on the broadband remote access server (BRAS) or L2TP access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is enabled. The following commands were introduced or modified: **sessions pre-auth limit ignore**.



CHAPTER 24

PPPoE QinQ Support

The PPPoE QinQ Support feature installed at a subinterface level preserves VLAN IDs and segregates the traffic in different customer VLANs. Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs.

Prerequisites for PPPoE QinQ Support

- You have checked Cisco Feature Navigator at http://www.cisco.com/go/cfn to verify that your Cisco device and Cisco IOS XE release support this feature.
- You must be connected to an Ethernet device that supports double VLAN tag imposition/disposition or switching.

Information About PPPoE QinQ Support

PPPoE QinQ Support on Subinterfaces

The PPPoE QinQ Support feature adds another layer of IEEE 802.1Q tag (called "metro tag" or "PE-VLAN") to the 802.1Q tagged packets that enter the network. The purpose is to expand the VLAN space by tagging the tagged packets, thus producing a "double-tagged" frame. The expanded VLAN space allows service providers to offer assorted services on different VLANs. For example, certain customers can be provided Internet access on specific VLANs while other customers receive different services on other VLANs.

Generally the service provider’s customers require a range of VLANs to handle multiple applications. Service providers can allow their customers to use this feature to safely assign their own VLAN IDs on subinterfaces because these subinterface VLAN IDs are encapsulated within a service provider-designated VLAN ID for that customer. Therefore there is no overlap of VLAN IDs among customers, nor does traffic from different customers become mixed. The double-tagged frame is "terminated" or assigned on a subinterface through use

of an expanded **encapsulation dot1q** command that specifies the two VLAN ID tags (outer VLAN ID and inner VLAN ID) terminated on the subinterface. See .

The PPPoE QinQ Support feature is generally supported on whichever Cisco IOS XE features or protocols are supported on the subinterface. For example, if you can run PPPoE on the subinterface, you can configure a double-tagged frame for PPPoE. IPoQinQ supports IP packets that are double-tagged for QinQ VLAN tag termination by forwarding IP traffic with the double-tagged (also known as stacked) 802.1Q headers.

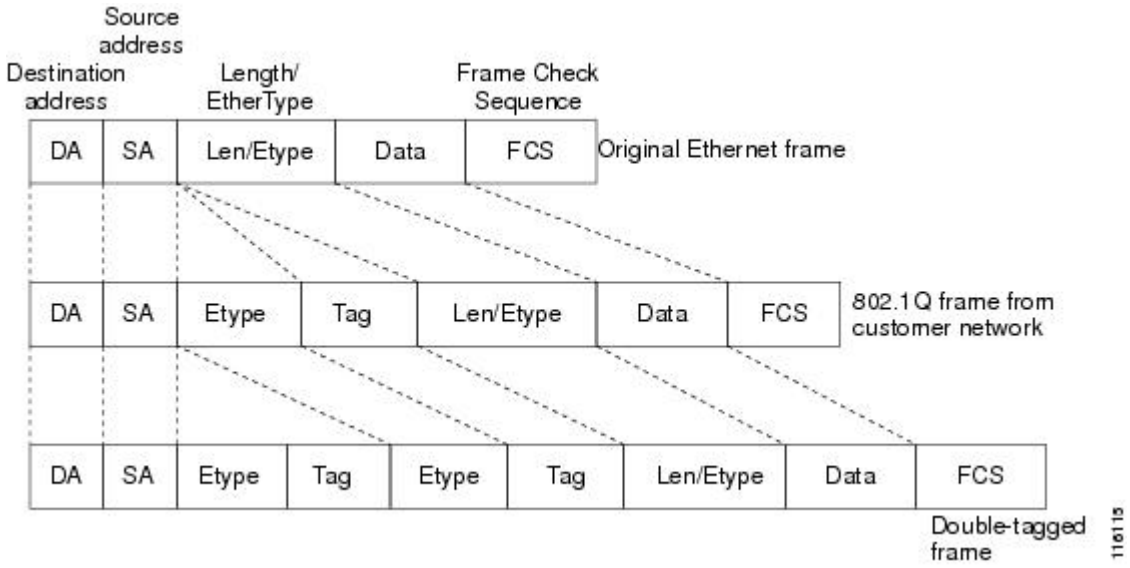
A primary consideration is whether you assign ambiguous or unambiguous subinterfaces for the inner VLAN ID. See the Unambiguous and Ambiguous Subinterfaces, on page 265.

The primary benefit for the service provider is a reduced number of VLANs supported for the same number of customers. Other benefits of this feature are as follows:

- PPPoE scalability. Expanding the available VLAN space from 4096 to about 16.8 million (4096 times 4096) allows the number of PPPoE sessions that can be terminated on a given interface to be multiplied.
- When deploying Gigabyte Ethernet DSL access multiplexer (DSLAM) in a wholesale model, you can assign the inner VLAN ID to represent the end-customer virtual circuit (VC) and assign the outer VLAN ID to represent the service provider ID.

The QinQ VLAN tag termination feature is simpler than the IEEE 802.1Q tunneling feature deployed for switches. Whereas switches require IEEE 802.1Q tunnels on interfaces to carry double-tagged traffic, routers need only encapsulate QinQ VLAN tags within another level of 802.1Q tags in order for the packets to arrive at the correct destination.

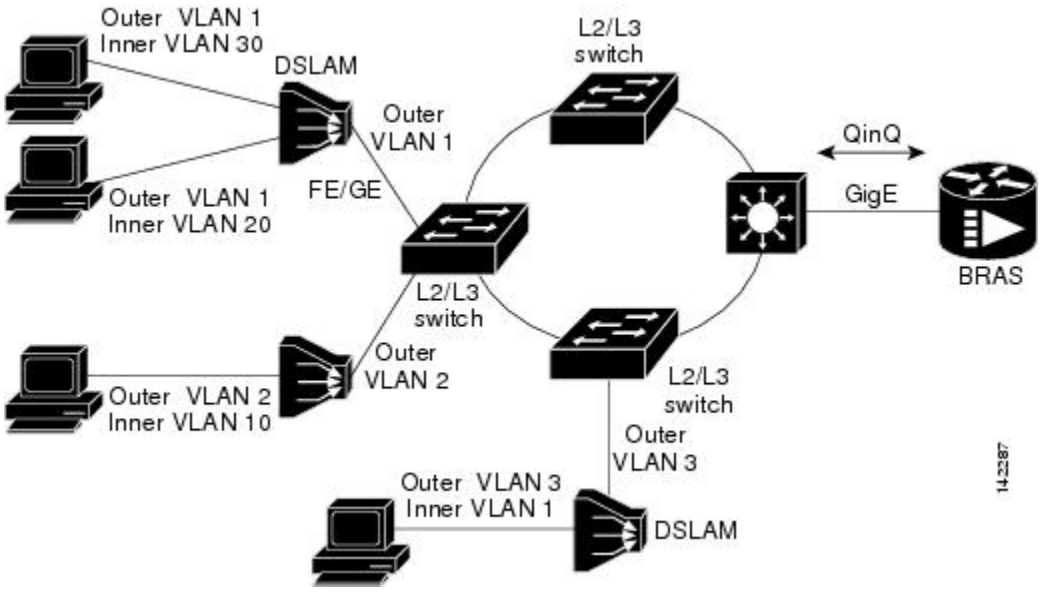
Figure 20: Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames



Broadband Ethernet-Based DSLAM Model of QinQ VLANs

For the emerging broadband Ethernet-based DSLAM market, the Cisco ASR 1000 Series Routers support QinQ encapsulation. With the Ethernet-based DSLAM model shown in the figure below, customers typically get their own VLAN; all these VLANs are aggregated on a DSLAM.

Figure 21: Broadband Ethernet-Based DSLAM Model of QinQ VLANs



VLAN aggregation on a DSLAM will result in many aggregate VLANs that at some point need to be terminated on the broadband remote access servers (BRASs). Although the model could connect the DSLAMs directly to the BRAS, a more common model uses the existing Ethernet-switched network where each DSLAM VLAN ID is tagged with a second tag (QinQ) as it connects into the Ethernet-switched network.

Both PPPoE sessions and IP can be enabled on a subinterface. The PPPoEoQinQ model is a PPP-terminated session.

PPPoEQinQ and IPoQinQ encapsulation processing is an extension to 802.1Q encapsulation processing. A QinQ frame looks like a VLAN 802.1Q frame; the only difference is that it has two 802.1Q tags instead of one.

QinQ encapsulation supports configurable outer tag Ethertype. The configurable Ethertype field values are 0x8100 (default), 0x9100, 0x9200, and 0x8848. See the figure below.

Figure 22: Supported Configurable Ethertype Field Values

Unambiguous and Ambiguous Subinterfaces

Note Only PPPoE is supported on ambiguous subinterfaces. Standard IP routing is not supported on ambiguous subinterfaces.

The **encapsulation dot1q** command is used to configure QinQ termination on a subinterface. The command accepts an outer VLAN ID and one or more inner VLAN IDs. The outer VLAN ID always has a specific value, and the inner VLAN ID can either be a specific value or a range of values.

A subinterface that is configured with a single inner VLAN ID is called an unambiguous QinQ subinterface. In the following example, QinQ traffic with an outer VLAN ID of 101 and an inner VLAN ID of 1001 is mapped to the Gigabit Ethernet 1/1/0.100 subinterface:

```
Router(config)# interface gigabitethernet1/1/0.100
Router(config-subif)# encapsulation dot1q 101 second-dot1q 1001
```

A subinterface that is configured with multiple inner VLAN IDs is called an ambiguous QinQ subinterface. By allowing multiple inner VLAN IDs to be grouped, ambiguous QinQ subinterfaces allow for a smaller configuration, improved memory usage, and better scalability.

In the following example, QinQ traffic with an outer VLAN ID of 101 and inner VLAN IDs anywhere in the 2001-2100 and 3001-3100 range is mapped to the Gigabit Ethernet 1/1/0.101 subinterface:

```
Router(config)# interface gigabitethernet1/1/0.101
Router(config-subif)# encapsulation dot1q 101 second-dot1q 2001-2100,3001-3100
```

Ambiguous subinterfaces can also use the **any**keyword to specify the inner VLAN ID.

See the Configuration Examples for PPPoE QinQ Support, on page 271 for an example of how VLAN IDs are assigned to subinterfaces, and for a detailed example of how the **any** keyword is used on ambiguous subinterfaces.

Note The **any** keyword in the **second-dot1q**keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. Therefore, multiple values and ranges for the inner VLAN ID are not supported on IPoQinQ.

How to Configure PPPoE QinQ Support

Configuring the Interfaces for PPPoE QinQ Support

Perform this task to configure the main interface used for the QinQ double tagging and to configure the subinterfaces. An optional step in this task shows you how to configure the Ethertype field to be 0x9100 for the outer VLAN tag, if that is required. After the subinterface is defined, the 802.1Q encapsulation is configured to use the double tagging.

Before you begin

- PPPoE or IP is already configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* /*subslot*/*port*
4. **dot1q tunneling ethertype** *ethertype*
5. **exit**
6. **interface** *type slot* /*subslot*/*port*[.*subinterface*]

7. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*| *vlan-id* **-** *vlan-id*[**,** *vlan-id* **-** *vlan-id*]}
8. **pppoe enable** [**group** *group-name*]
9. **ip address** *ip-address mask* [**secondary**]
10. **exit**
11. Repeat Step 6 to configure another subinterface.
12. Repeat Step 7, Step 8, and Step 9, as required, to specify the VLAN tags to be terminated on the subinterface.
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* /*subslot*/*port* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**dot1q tunneling ethertype** *ethertype* **Example:** `Router(config-if)# dot1q tunneling ethertype 0x9100`	(Optional) Defines the Ethertype field type used by peer devices when implementing QinQ VLAN tagging. • Use this command if the Ethertype of peer devices is 0x9100 or 0x9200.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.
Step 6	**interface** *type slot* /*subslot*/*port*[.*subinterface*] **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.1`	Configures a subinterface and enters subinterface configuration mode.
Step 7	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*| *vlan-id* **-** *vlan-id*[**,** *vlan-id* **-** *vlan-id*]} **Example:**	(Required) Enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.

	Command or Action	Purpose
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	• Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface. • In this example, an unambiguous QinQ subinterface is configured because only one inner VLAN ID is specified. • QinQ frames with an outer VLAN ID of 100 and an inner VLAN ID of 200 will be terminated.
Step 8	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group vpn1`	(Optional) Enables PPPoE sessions on a subinterface. • The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface. **Note** This step is required only for PPPoEoQinQ.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 192.168.1.2 255.255.255.0`	(Optional) Sets a primary or secondary IP address for a subinterface. • The example enables IP on the subinterface specified by the IP address, 192.168.1.2, and mask, 255.255.255.0. **Note** This step is required only for IPoQinQ.
Step 10	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.
Step 11	Repeat Step 6 to configure another subinterface. **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.2`	(Optional) Configures a subinterface and enters subinterface configuration mode.

Step 12	Repeat Step 7, Step 8, and Step 9, as required, to specify the VLAN tags to be terminated on the subinterface.
	Example:
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600`
	Example:
	`Router(config-subif)# pppoe enable group vpn1`
	Example:
		Specifies the VLAN tags to be terminated on the subinterface, to enable PPPoE sessions or IP on the subinterface.
		• Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface.
		• In the example, an ambiguous QinQ subinterface is configured because a range of inner VLAN IDs is specified.

	Command or Action	Purpose
	`Router(config-subif)# ip address 192.168.1.2 255.255.255.0`	• QinQ frames with an outer VLAN ID of 100 and an inner VLAN ID in the range of 100 to 199 or 201 to 600 will be terminated. • Step 7 enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. • Step 8 enables PPPoE sessions on the subinterface. The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface. • Step 9 enables IP on a subinterface specified by the IP address and mask. The example enables IP on the subinterface specified by the IP address, 192.168.1.2, and mask, 255.255.255.0. **Note** Both PPPoE sessions and IP can be enabled on a subinterface.
Step 13	**end** **Example:** `Router(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Verifying the PPPoE QinQ Support

Perform this optional task to verify the configuration of the PPPoE QinQ Support feature.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show vlans dot1q** [**internal** | *interface-type interface-number.subinterface-number*[**detail**] | *outer-id*[*interface-type interface-number* | **second-dot1q** [*inner-id*| **any**]] [**detail]**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show running-config**

Use this command to show the currently running configuration on the device. You can use delimiting characters to display only the relevant parts of the configuration.

The following output shows the currently running PPPoEoQinQ and IPoQinQ configurations:

Example:

```
Router# show running-config
interface GigabitEthernet0/0/0.201
 encapsulation dot1Q 201
 ip address 10.7.7.5 255.255.255.252
!
interface GigabitEthernet0/0/0.401
 encapsulation dot1Q 401
 ip address 10.7.7.13 255.255.255.252
!
interface GigabitEthernet0/0/0.201999
 encapsulation dot1Q 201 second-dot1q any
 pppoe enable
!
interface GigabitEthernet0/0/0.2012001
 encapsulation dot1Q 201 second-dot1q 2001
 ip address 10.8.8.9 255.255.255.252
!
interface GigabitEthernet0/0/0.2012002
 encapsulation dot1Q 201 second-dot1q 2002
 ip address 10.8.8.13 255.255.255.252
 pppoe enable
!
interface GigabitEthernet0/0/0.4019999
 encapsulation dot1Q 401 second-dot1q 100-900,1001-2000
 pppoe enable
!
interface GigabitEthernet1/0/0.101
 encapsulation dot1Q 101
 ip address 10.7.7.1 255.255.255.252
!
interface GigabitEthernet1/0/0.301
 encapsulation dot1Q 301
 ip address 10.7.7.9 255.255.255.252
!
interface GigabitEthernet1/0/0.301999
 encapsulation dot1Q 301 second-dot1q any
 pppoe enable
!
interface GigabitEthernet1/0/0.1011001
 encapsulation dot1Q 101 second-dot1q 1001
 ip address 10.8.8.1 255.255.255.252
!
interface GigabitEthernet1/0/0.1011002
 encapsulation dot1Q 101 second-dot1q 1002
 ip address 10.8.8.5 255.255.255.252
!
interface GigabitEthernet1/0/0.1019999
 encapsulation dot1Q 101 second-dot1q 1-1000,1003-2000
 pppoe enable
```

Step 3 **show vlans dot1q** [**internal** | *interface-type interface-number.subinterface-number*[**detail**] | *outer-id*[*interface-type interface-number* | **second-dot1q** [*inner-id*| **any**]] [**detail]**]

Use this command to show the statistics for all the 802.1Q VLAN IDs. In the following example, only the outer VLAN ID is displayed:

Note The **any** keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces.

Example:

```
Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

Configuration Examples for PPPoE QinQ Support

Configuring the any Keyword on Subinterfaces for PPPoE QinQ Support Example

Some ambiguous subinterfaces can use the **any** keyword for the inner VLAN ID specification. The **any** keyword represents any inner VLAN ID that is not explicitly configured on any other interface. In the following example, seven subinterfaces are configured with various outer and inner VLAN IDs.

Note The **any** keyword can be configured on only one subinterface of a specified physical interface and outer VLAN ID.

Note The **any** keyword in the **second-dot1q**keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. Therefore, multiple values and ranges for the inner VLAN ID are not supported on IPoQinQ.

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
interface GigabitEthernet1/0/0.3
 encapsulation dot1q 100 second-dot1q 300-400,500-600
interface GigabitEthernet1/0/0.4
 encapsulation dot1q 100 second-dot1q any
interface GigabitEthernet1/0/0.5
 encapsulation dot1q 200 second-dot1q 50
interface GigabitEthernet1/0/0.6
 encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000
interface GigabitEthernet1/0/0.7
 encapsulation dot1q 200 second-dot1q any
```

The table below shows which subinterfaces are mapped to different values of the outer and inner VLAN IDs on QinQ frames that come in on Gigabit Ethernet (GE) interface 1/0/0.

Table 27: Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0

Outer VLAN ID	Inner VLAN ID	Subinterface Mapped to
100	1 through 99	GigabitEthernet1/0/0.4
100	100	GigabitEthernet1/0/0.1
100	101 through 199	GigabitEthernet1/0/0.4
100	200	GigabitEthernet1/0/0.2
100	201 through 299	GigabitEthernet1/0/0.4
100	300 through 400	GigabitEthernet1/0/0.3
100	401 through 499	GigabitEthernet1/0/0.4
100	500 through 600	GigabitEthernet1/0/0.3
100	601 through 4094	GigabitEthernet1/0/0.4
200	1 through 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 through 999	GigabitEthernet1/0/0.7
200	1000 through 2000	GigabitEthernet1/0/0.6
200	2001 through 2999	GigabitEthernet1/0/0.7
200	3000 through 4000	GigabitEthernet1/0/0.6
200	4001 through 4094	GigabitEthernet1/0/0.7

A new subinterface is now configured:

```
interface GigabitEthernet 1/0/0.8
 encapsulation dot1q 200 second-dot1q 200-600,900-999
```

The table below shows the changes made to the table for the outer VLAN ID of 200. Notice that subinterface 1/0/0.7 configured with the **any** keyword now has new inner VLAN ID mappings.

Table 28: Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0--Changes Resulting from Configuring GE Subinterface 1/0/0.8

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
200	1 through 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 through 199	GigabitEthernet1/0/0.7

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
200	200 through 600	GigabitEthernet1/0/0.8
200	601 through 899	GigabitEthernet1/0/0.7
200	900 through 999	GigabitEthernet1/0/0.8
200	1000 through 2000	GigabitEthernet1/0/0.6
200	2001 through 2999	GigabitEthernet1/0/0.7
200	3000 through 4000	GigabitEthernet1/0/0.6
200	4001 through 4094	GigabitEthernet1/0/0.7

Additional References

The following sections provide references related to the PPPoE QinQ Support feature.

Related Documents

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* •

Standards

Standards	Title
IEEE 802.1Q	IEEE Standard for Local and Metropolitan Area Networks

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

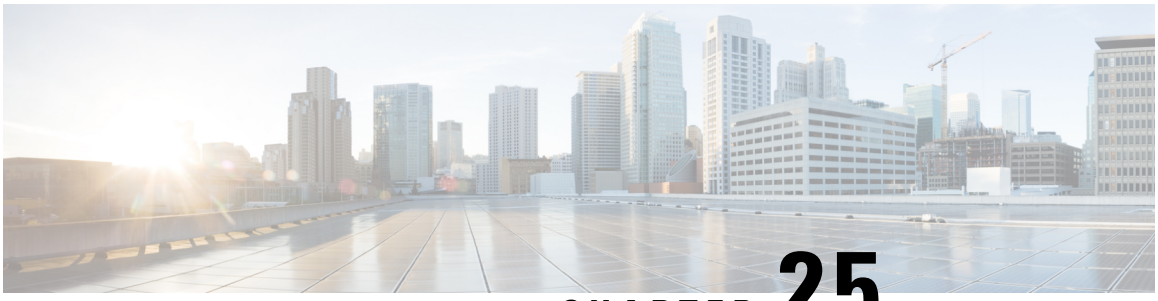
Feature Information for PPPoE QinQ Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 29: Feature Information for PPPoE QinQ Support

Feature Name	Releases	Feature Information
IEEE 802.1Q-in-Q VLAN Tag Termination	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs.
PPPoE QinQ Support	Cisco IOS XE Release 2.2	This feature was introduced on Cisco ASR 1000 Series Routers. This feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated. The following commands were introduced or modified: **dot1q tunneling ethertype**, **encapsulation dot1q**, **show vlans dot1q**.



CHAPTER 25

TR-069 Agent

The digital subscriber line (DSL) Forum's TR-069, CPE WAN Management Protocol (CWMP), is used for communications between a customer premise equipment (CPE) and an auto-configuration server (ACS). The TR-069 Agent feature manages a collection of CPEs, with the primary capability for auto-configuration and dynamic service provisioning, software image management, status and performance monitoring and diagnostics.

Information About the TR-069 Agent

Limitations for the TR-069 Agent

The following table provide the limitations of the parameters in TR-069.

Table 30: TR-069 Parameters

TR-069 Parameter	Expected Value	Supported on Cisco ISR G2	Supported on Cisco 4451
InternetGatewayDevice. WANDevice.2. WANConnectionDevice.WANPPPConnection	Time	No	No

TR-069 Parameter	Expected Value	Supported on Cisco ISR G2	Supported on Cisco 4451
Internet gatewy device. WAN device2. WAN common interface config enabled. For Internet registration entry for Internet gateway device. WAN device. WAN common Interface configuration does not include the parameter enabled for Internet.	True or Flase	No	No
[illegible] for the Cisco ISR4451 Chassis is NULL, hence [illegible] is also NULL	Version	Yes	No
WAN access type is DSL (Internet gateway device. WAN device2. WAN common interface configuration. WAN access type) The WAN DSL interface configuration data is populates when the WAN access type is Ethernet (Internet Gateway device. WAN device. WAN common interface configuration interface config. WAN access type). The WAN Ethernet interface configuration date populates.	Populate the details	Yes	Yes
[illegible] entry for [illegible] does not include the parameter MTU	MTU value	No	No

TR-069 Parameter	Expected Value	Supported on Cisco ISR G2	Supported on Cisco 4451
Internet gateway device. Layer 3 forwarding. Forwarding 1. MTU registration entry for Internet gateway device. Layer 3 forwarding. Forwarding does not include the parameter MTU.	MTU value	No	No
Set parameter values-Internet gateway device. Time. NTP server 5 in Cisco 4451, config t, archive, path boot flash should be configured to set the value in Cisco ISR G2; only one storage path and it is the flash memory.	ntp server 100.12.12.1	YES (no archive)	YES (configure archive)

TR-069 Agent

The TR-069 Agent allows an ACS to provision a CPE or collection of CPEs. The provisioning mechanism includes specific provisioning parameters and a general mechanism for adding vendor-specific provisioning capabilities as needed. The identification mechanisms included in the protocol allow CPE provisioning based either on the requirements of each specific CPE, or on collective criteria such as the CPE vendor, model, software version, or other criteria.

The provisioning mechanism allows CPE provisioning at the time of initial connection to the broadband access network and the ability to reprovision at any subsequent time. This includes support for asynchronous ACS-initiated reprovisioning of a CPE.

The TR-069 Agent also supports image upgrade, configuration application, file downloads, configuration and log file uploads, and CPE monitoring.

Note The TR-069 Agent CPE devices must be set up and enabled for TR-069. An ACS used to communicate with the CPE must be TR-069 compliant in order to enable the TR-069 Agent.

RPC Support

The following remote procedure calls (RPCs) are supported with the TR-069 Agent:

- Standard RPCs
  - GetRPCMethods
  - SetParameterValues

- GetParameterValues
- GetParameterNames
- SetParameterAttributes
- GetParameterAttributes
- AddObject
- DeleteObject
- Reboot
- Download
- Upload

Note In case of the Download operation, the file transfer option is supported only through HTTP.

- Vendor RPCs
  - X_00000C_SetConfiguration
  - X_00000C_ShowStatus

CWMP Vendor Profile Schema

The following details the CWMP vendor profile schema:

- For SetConfiguration,

```
<cwmp:X_00000C_SetConfiguration>
<ErrorOption> rollback </ErrorOption>
<Target> {running-config | startup-config} </Target>
<ConfigCommandBlock> block of clis separated by newline [\n] character </ConfigCommandBlock>
<ConfigCommandList array of strings[1..unbounded] each of length 256>
<string> IOS Configuration command 1 </string>
<string> IOS Configuration command 2 </string>
</ConfigCommandList>
<ParameterKey> parameterkey </ParameterKey>
</cwmp:X_00000C_SetConfiguration>

ErrorOption => string with length 64
Target => string with length 64
```

On success,

```
<X_00000C_SetConfigurationResponse>
<Status>0</Status>
</X_00000C_SetConfigurationResponse>
```

On failure,

```
<SOAP:Fault>
<SOAP:faultcode>Client</SOAP:faultcode>
<SOAP:faultstring>CWMP fault</SOAP:faultstring>
<SOAP:detail>
<cwmp:Fault>
<FaultCode></FaultCode>
<FaultString></FaultString>

<cwmp:X_00000C_SetConfigurationFault>
<Command>IOS Configuration command that failed</Command>
<FaultCode>parse_cmd() return value</FaultCode>
</cwmp:X_00000C_SetConfigurationFault>

<cwmp:X_00000C_SetConfigurationFault>
<Command>IOS Configuration command that failed</Command>
<FaultCode>parse_cmd() return value</FaultCode>
</cwmp:X_00000C_SetConfigurationFault>

</cwmp:Fault>
</SOAP:detail>
</SOAP:Fault>
```

- For ShowStatus,

```
<cwmp:X_00000C_ShowStatus>
<ExecCommandList array of strings[1..unbounded] each of length 256 >
<string> IOS Exec command 1 </string>
<string> IOS Exec command 2 </string>
<string> IOS Exec command 3 </string>
</ExecCommandList>
</cwmp:X_00000C_ShowStatus>
```

On success,

```
<cwmp:X_00000C_ShowStatusResponse>
<ExecResponseList array of ExecResponseStruct [1..unbounded]>
<ExecResponseStruct>
<Command> IOS Exec command 1 </Command>
<Response> output of command 1</Response>
</ExecResponseStruct>

<ExecResponseStruct>
<Command> IOS Exec command 2 </Command>
<Response> output of command 2 </Response>
</ExecResponseStruct>

<ExecResponseStruct>
<Command> IOS Exec command 3 </Command>
<Response>output of command 3</Response>
</ExecResponseStruct>

</ExecResponseList>
</cwmp:X_00000C_ShowStatusResponse>
```

On failure,

```
<SOAP:Fault>
<SOAP:faultcode>Client</SOAP:faultcode>
<SOAP:faultstring>CWMP fault</SOAP:faultstring>
```

```
<SOAP:detail>
<cwmp:Fault>
<FaultCode></FaultCode>
<FaultString></FaultString>
</cwmp:Fault>
</SOAP:detail>
</SOAP:Fault>
```

HTTP Digest Authentication Support

The TR-069 Agent uses HTTP as the transport and needs support for digest authentication from the HTTP client infrastructure.

Note This feature is not a TR-069 Agent-exclusive feature and can be used in other scenarios to configure HTTP Digest Authentication Support.

HTTP Cookie Support Per RFC2965

A cookie is a piece of HTTP state information generated and sent by an HTTP server in response to an HTTP request. The HTTP client returns the cookie containing the state information back to the HTTP server in its next HTTP request. This scenario is used to create a stateful session with HTTP requests and responses. The TR-069 Agent uses HTTP as the transport and needs support for both Netscape cookies and RFC 2965 in HTTP client infrastructure.

Note This feature is not a TR-069 Agent-exclusive feature and can be used in other scenarios to clear, monitor and troubleshoot HTTP cookies.

Device Gateway Association

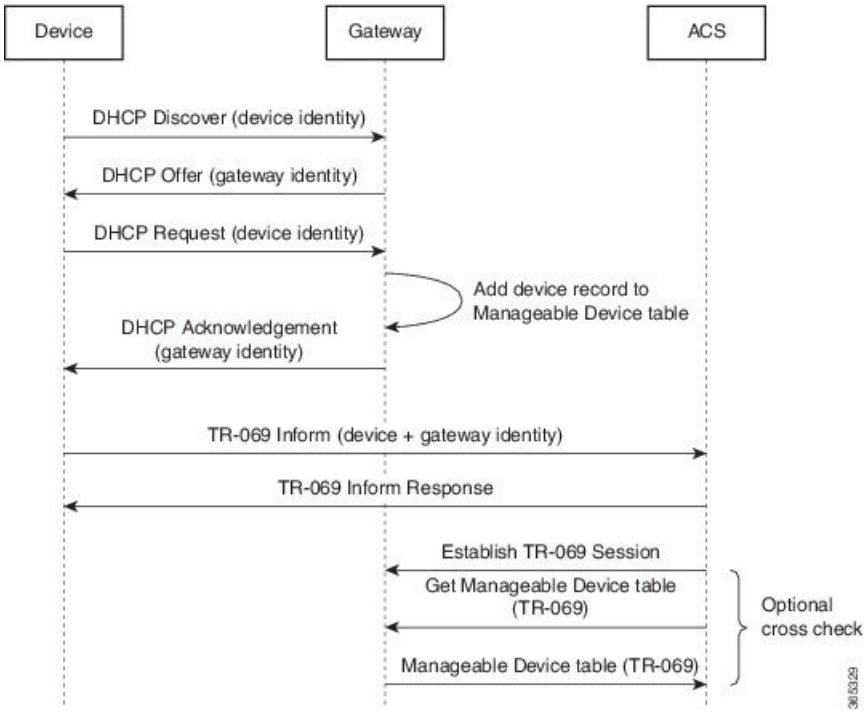
The CPE WAN Management Protocol (CWMP) can be used to remotely manage customer premise equipment (CPE) devices that are connected over a LAN through a gateway. If Auto Configuration Server (ACS) manages both the Device and the Gateway through which the device is connected , ACS determines the identity of the gateway by checking the device gateway association information. The ACS with the device gateway association profile can identify the end devices behind each gateway. The device gateway association constitutes Annex F (previously part of TR-111), part of the TR-069 standard. The mechanism defined for device gateway association relies on the Device's use of Dynamic Host Configuration Protocol (DHCP) Option 125. The end devices will pass on their identity to the gateway via vendor-specific DHCP option. When the gateway receives this information, the gateway populates the ManageableDevice table containing identity information for each device on its LAN. The parameters, which are supported on the gateway as part of device gateway association is as follows:

- **InternetGatewayDevice.ManagementServer.ManageableDeviceNumberOfEntries**
- **InternetGatewayDevice.ManagementServer.ManageableDevice.{i}**
  - **ManufacturerOUI**
  - **ProductClass**

- **SerialNumber**

The device gateway association functionality does not support configuring IP addresses manually on the end devices. The IP addresses are assigned to the end devices via DHCP by the gateway. You must configure **renew deny unknown** command under the DHCP server configuration to initiate the DHCP discovery process for the end devices after a gateway reload.

Figure 23: Device-Gateway Association using DHCP Discover



The following example shows how to set up the Device-Gateway Association and Port Mapping feature via a Dynamic Host Configuration Protocol (DHCP) on VLAN interface:

```
ip dhcp excluded-address 15.15.15.1
!
ip dhcp pool NET-POOL1
 network 15.15.15.0 255.255.255.0
 default-router 15.15.15.1
 lease 0 0 5
 renew deny unknown
 end
 interface Vlan102
  ip address pool NET-POOL1
  end
```

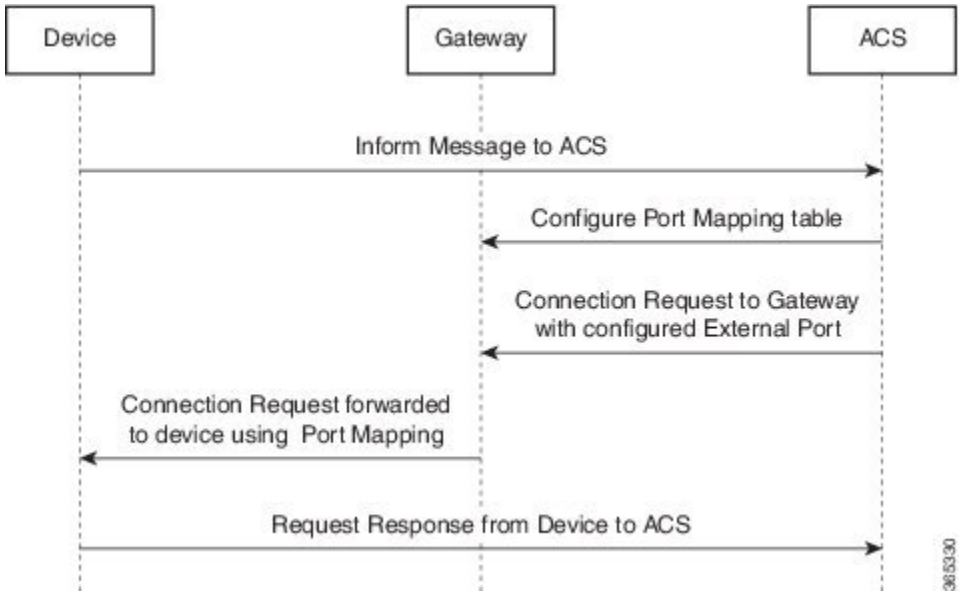
Port Mapping Support

The CPE WAN Management Protocol (CWMP) can be used to remotely manage customer premise equipment (CPE) devices that are connected via a LAN through a network address translation (NAT) gateway. This can be achieved by making use of the PortMapping functionality. This feature helps in maintaining the privacy of the IP addresses of the end devices as the communication happens with the auto-configuration server (ACS) in the public domain. The gateway supports the following CWMP parameters:

- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.PortMappingNumberOfEntries**
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Port-Mapping.{i}.**
  - **PortMappingEnabled**
  - **PortMappingLeaseDuration**
  - **RemoteHost**
  - **ExternalPort**
  - **InternalPort**
  - **PortMappingProtocol**
  - **InternalClient**
  - **PortMappingDescription**
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPP-Connection.{i}.PortMappingNumberOfEntries**
- **InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPP-Connection.{i}.PortMapping.{i}.**
  - **PortMappingEnabled**
  - **PortMappingLeaseDuration**
  - **RemoteHost**
  - **ExternalPort**
  - **InternalPort**
  - **PortMappingProtocol**
  - **InternalClient**
  - **PortMappingDescription**

Note The ACS must provide values for the mandatory parameters—**ExternalPort**, **InternalPort**, **PortMappingProtocol**, and **InternalClient**—to the gateway for adding the port mapping for an end device. There is no support to limit the portmapping to a particular host using **RemoteHost** parameter.

Figure 24: Connection request via a NAT Gateway using PortMapping table



The following is an example Port Mapping Support on a device configured as a gateway and ACS.

For the below parameters configured on ACS,

```
Destination IP (InternalClient) - 15.15.15.2
Source port (ExternalPort)  - 9000
Destination port (InternalPort) - 7547
PortMappingProtocol - TCP
```

the following NAT command is configured on the gateway:

```
ip nat inside source static tcp 15.15.15.2 7547 10.194.145.170 9000 extendable
```

10.194.145.170 is the RemoteHost and the IP address of the device or gateway provisioned by ACS. This is the IP address corresponding to the interface with the configuration **cwmp wan default** command.

VRF Support for CPE WAN Management Protocol

The digital subscriber line (DSL) forum's TR-069 and CPE WAN Management Protocol (CWMP) are used for communications between a customer premise equipment (CPE) and an auto-configuration server (ACS). Virtual Route Forward (VRF) will be supported on TR-069 and TR-111 from Cisco IOS XE Bengaluru 17.4.1 onwards.

This feature supports:

- TR-069 within a VRF aware interface
- TR-069 within a VRF aware sub-interface
- TR-069 within a VRF aware loopback interface
- Device association profile over VRF
- Port mapping table over VRF
- Port forwarding service from ACS

The following are the examples for different scenarios:

TR069 within a VRF: WAN IP over Interface

```
interface GigabitEthernet0/0/1
vrf forwarding blue
ip address 11.1.1.1 255.255.255.0
cwmp wan default
```

TR069 within a VRF: WAN IP over Sub-interface

```
interface GigabitEthernet0/0/1.4092
encapsulation dot1Q 4092
vrf forwarding blue
ip address 12.1.1.1 255.255.255.0
cwmp wan default
```

TR069 within a VRF: Loopback IP over Interface

```
interface GigabitEthernet0/0/1
vrf forwarding blue
ip address 11.1.1.1 255.255.255.0


interface Loopback0
vrf forwarding blue
ip address 20.1.1.1 255.255.255.0
cwmp wan default
```

TR069 within a VRF: WAN IP Assigned through DHCP over Sub-interface

```
interface GigabitEthernet0/0/1.4092
encapsulation dot1Q 4092
vrf forwarding blue
ip address dhcp
cwmp wan default

On peer end, ip dhcp pool should be configured as follows:

ip dhcp excluded-address 12.1.1.2
ip dhcp pool cwmp-pool
network 12.1.1.0 255.255.255.0
default-router 12.1.1.2
```

Device-Gateway Association Profile Parameters

```
Router#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name

Bindings from VRF pool blue:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
5.6.6.2        0004.137a.1c50         Mar 04 2020 04:33 PM    Automatic  Active     Vlan102
5.6.6.3        0004.137a.1c7a         Mar 04 2020 04:33 PM    Automatic  Active     Vlan102
Router#sh ip dhcp binding vrf blue

Bindings from VRF pool blue:
```

```
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
5.6.6.2         0004.137a.1c50          Mar 04 2020 04:33 PM    Automatic  Active     Vlan102
5.6.6.3         0004.137a.1c7a          Mar 04 2020 04:33 PM    Automatic  Active     Vlan102

Router#show cwmp map wandevice
CWMP WAN Id     Interface
1               GigabitEthernet0/0/1
```

Port Mapping Table Support over Sub-interface

```
interface GigabitEthernet0/0/1.4092
 encapsulation dot1Q 4092
 vrf forwarding blue
 ip address 12.1.1.1 255.255.255.0
 ip nat outside

cwmp wan default
interface GigabitEthernet0/1/7
 switchport access vlan 102
interface Vlan102
vrf forwarding blue
 ip address 5.6.6.1 255.255.255.0
  ip nat inside

On UUT, NAT should be configured as follows:

ip access-list extended NATLIST
permit ip 5.6.6.0 0.0.0.255 any
ip nat inside source list NATLIST interface GigabitEthernet0/0/1.4092 vrf blue overload
```

How to Configure and Enable the TR-069 Agent

Setting Up the CPE to Communicate with the ACS

Perform this task and the following tasks to configure and enable the TR-069 agent on the CPE. If an Ethernet or Serial interface is used to communicate with ACS, these tasks need not be performed manually because the tasks are automated by using the AutoInstall feature. For more information on the AutoInstall feature, refer to *Using AutoInstall to Remotely Configure Cisco Networking Devices*. For an example on configuring CWMP with the autoinstall feature, see the *Example: Configuring and Enabling CWMP using the Autoinstall feature* section.

Before you begin

If the ACS URL is an HTTP URL, enable the Cisco IOS HTTP Server using the **ip http server**command. If the ACS URL is an HTTPS URL, enable the Cisco IOS HTTP Secure Server using the **ip http secure-server** command. For more information about the **ip http server** and **ip http secure-server** commands, refer to the *Cisco IOS Network Management Command Reference*.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **cwmp agent**
4. **management server url** *acs-url*
5. **management server password** [*encryption-type* | *cleartext-password*] *passwd*
6. **provision code** *code-string*
7. **exit**
8. **interface** *type number*
9. **cwmp wan**
10. **cwmp wan default**
11. **exit**
12. **cwmp agent**
13. **enable download**
14. **session retry limit** *session-count*
15. **request outstanding** *request-count*
16. **parameter change notify interval** *time-interval*
17. **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	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.

Step 4	**management server url** *acs-url*
	Example:
	`Device(config-cwmp)# management server url http://172.25.117.78:7547/acs`
	Example:
	`Device(config-cwmp)# management server url https://172.25.117.78:7547/acs`
		Specifies the HTTP/HTTPS URL to reach the ACS. This URL is used by the CPE to establish the TR-069 session with the ACS.

Step 5	**management server password** [*encryption-type* | *cleartext-password*] *passwd*	Specifies the CPE password that is used in the authentication phase.

	Command or Action	Purpose
	Example: `Device(config-cwmp)# management server password 0 cisco`	• This password will be provided to the ACS when the CPE is challenged for credential as part of authentication during the session establishment.
Step 6	**provision code** *code-string* **Example:** `Device(config-cwmp)# provision code ABCD`	Specifies the provision code to be used by the CPE.
Step 7	**exit** **Example:** `Device(config-cwmp)# exit`	Exits TR-069 Agent configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device# interface serial 0/0`	Enters interface configuration mode.
Step 9	**cwmp wan** **Example:** `Device(config-if)# cwmp wan`	(Optional) Defines the WAN interfaces on the CPE. **Note** Any interface without this command is considered a LAN interface by TR-069 protocol. There can be multiple WAN and LAN interfaces configured on the CPE. By default, an ATM interface on the CPE will be considered a WAN interface by the TR-069 protocol.
Step 10	**cwmp wan default** **Example:** `Device(config-if)# cwmp wan default`	Defines the default WAN interfaces on the CPE device. **Note** Among the multiple WAN interfaces, there can be only one default WAN interface in which the TR-069 communication could happen. If you try to configure this command on multiple interfaces, only the latest configuration will be active and the previous default WAN interface will become a WAN interface, ensuring only one interface is the default at any point in time.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 12	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.

	Command or Action	Purpose
Step 13	**enable download** **Example:** `Device(config-cwmp)# enable download`	(Optional) Enables the CPE to permit a software download. By default, this command is disabled.
Step 14	**session retry limit** *session-count* **Example:** `Device(config-cwmp)# session retry limit 10`	(Optional) Sets the session retry count whenever the TR-069 session establishment fails with the ACS. • The range for the session count argument is 0 to 15. • The default value is 11.
Step 15	**request outstanding** *request-count* **Example:** `Device(config-cwmp)# request outstanding 6`	(Optional) Sets the count for the number of requests that can be sent by CPE to ACS without receiving the acknowledgement. • The range for the request count argument is 0 to 10. • The default value is 5.
Step 16	**parameter change notify interval** *time-interval* **Example:** `Device(config-cwmp)# parameter change notify interval 75`	(Optional) Sets the time interval, in seconds, for the parameter change notifications. • The range for the time interval argument is 15 to 300. • The default value is 60.
Step 17	**end** **Example:** `Device(config-cwmp)# end`	Exits TR-069 Agent configuration mode and returns to privileged EXEC mode.

What to do next

Proceed to *Enabling the TR-069 Agent on the CPE* task.

Initiating a TR-069 Agent Session from the ACS

Before you begin

You must have set up the CPE by using *Setting Up the CPE to Communicate with the ACS* task and enabled the TR-069 Agent on the CPE by using the *Enabling the TR-069 Agent on the CPE* task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cwmp agent**
4. **connection request username** *username*
5. **connection request username [** *encryption-type* | *cleartext-password*] *passwd*

6. **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	**cwmp agent** **Example:** `Device(config)# cwmp agent`	Enables TR-069 Agent configuration mode.
Step 4	**connection request username** *username* **Example:** `Device(config-cwmp)# connection request username cisco`	Specifies the username used to authenticate an ACS which makes a connection request to a CPE.
Step 5	**connection request username [** *encryption-type* | *cleartext-password*] *passwd* **Example:** `Device(config-cwmp)# connection request password 0 cisco`	Specifies the password used to authenticate an ACS which makes a connection request to a CPE.
Step 6	**end** **Example:** `Device(config-cwmp)# end`	Exits TR-069 Agent configuration mode.

Configuring HTTP Digest Authentication Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http digest algorithm** *digest-algorithm*
4. **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	**ip http digest algorithm** *digest-algorithm* **Example:** `Device(config)# ip http digest algorithm md5`	Configures the MD5 digest algorithm parameter. • The choices for the digest algorithm parameter are MD5 and MD5-sess. • MD5 is the default.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Clearing the HTTP Cookies

Perform this task to clear the HTTP cookies.

SUMMARY STEPS

1. **enable**
2. **clear ip http client cookie** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name* **]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip http client cookie** [**domain** *cookie-domain*	**name** *cookie-name*	**session** *session-name* **]** **Example:** `Device# clear ip http client cookie name test`	Clears the HTTP cookies.

Monitoring and Troubleshooting the HTTP Cookies

SUMMARY STEPS

1. **enable**
2. **show ip http client cookie {brief | summary}** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name* **]**
3. **debug ip http cookie**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip http client cookie {brief | summary}** [**domain** *cookie-domain* | **name** *cookie-name* | **session** *session-name* **]** **Example:** `Device# show ip http client cookie brief name test`	Shows the HTTP cookies.
Step 3	**debug ip http cookie** **Example:** `Device# debug ip http cookie`	Troubleshoots the HTTP cookies.

Configuration Examples for TR-069 Agent

Example: Setting Up the CPE to Communicate with the ACS

The following example shows how to set up the CPE to communicate with the ACS. The ACS URL is http://172.25.117.78:7547/acs and the password is lab.

```
!
configure terminal
 cwmp agent
  management server url http://172.25.117.78:7547/acs
  management server password 0 lab
  provision code ABCD
  exit
 interface ethernet 0/0
  cwmp wan
  cwmp wan default
```

```
  exit
 cwmp agent
  enable download
  session retry limit 12
  request outstanding 3
  parameter change notify interval 120
!
```

Example: Configuring and Enabling CWMP using the Autoinstall feature

The following example shows how to configure CWMP using the autoinstall feature. Use the following set of commands in the network-config file or hostname-config file or router-config file in the TFTP server. No additional manual configuration is required for configuring CWMP on the device.

```
!
cwmp agent
 enable
 enable download
 management server password lab
 management server url http://10.1.98.229:7547/acs
 connection request username user1
 connection request password lab
!
ip http server
!
```

Additional References for TR-069 Agent

The following sections provide references related to the TR-069 Agent feature.

Related Documents

Related Topic	Document Title
TR-069 Agent commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

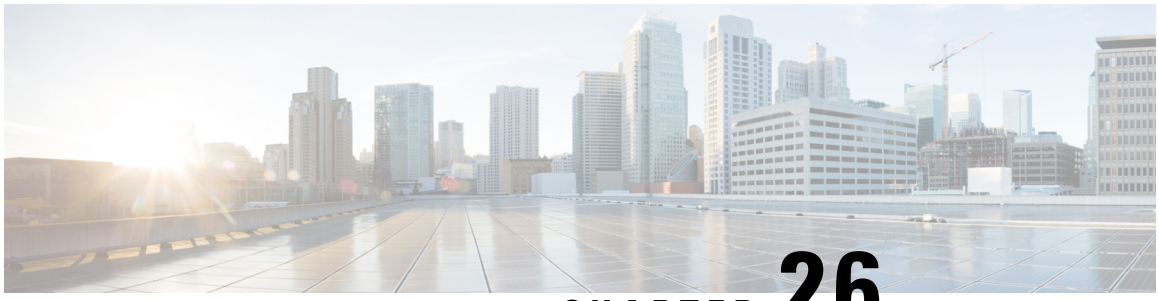
MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 26

PPP-Max-Payload and IWF PPPoE Tag Support

The PPP-Max-Payload and IWF PPPoE Tag Support feature enables the PPP over Ethernet (PPPoE) component to process the PPP-Max-Payload and Interworking Functionality (IWF) PPPoE tags in the PPPoE discovery frame:

- The **tag ppp-max-payload** command allows PPPoE peers to negotiate PPP maximum receive units (MRUs) greater than 1492 octets if the underlying network supports a maximum transmission unit (MTU) size greater than 1500 octets.
- The IWF PPPoE tag allows the Broadband Remote Access Server (BRAS) to distinguish the IWF PPPoE from the regular PPPoE sessions to overcome the per-MAC session limit put on the BRAS as a protection from denial of service (DOS) attacks sourced from the same MAC address.

Information About PPP-Max-Payload and IWF PPPoE Tag Support

Accommodating an MTU MRU Greater than 1492 in PPPoE

Per the RFC, "Accommodating an MTU/MRU Greater than 1492 in PPPoE," PPPoE peers can negotiate only MRUs with a maximum of 1492 octets so that the PPPoE header and PPP protocol ID can be inserted in the PPPoE session data packet. The maximum for an Ethernet payload is 1500 octets.

RFC 2516 defines a new tag to allow PPPoE peers to negotiate PPP MRU greater than 1492 if the underlying networks can support an Ethernet payload of greater than 1500 bytes. To enable processing of this new tag, a command has been defined in the Cisco IOS command-line interface as **tag ppp-max-payload.**The PPP-Max-Payload and IWF PPPoE Tag Support feature enhances the PPPoE component so the **tag ppp-max-payload**command can process the new tag to influence the Link Control Protocol (LCP) MRU negotiations for the PPP session based on the MRU value specified in the tag from the PPPoE client.

Interworking Functionality

The DSL Forum defined IWF to define the process for conversion of PPP over ATM (PPPoA) sessions to PPPoE sessions at the digital subscriber line access multiplexer (DSLAM) to the BRAS. This functionality was defined to help the migration of DSLAM networks from ATM to Ethernet media. So, essentially, the PPPoA session comes in to the DSLAM over ATM and is converted to a PPPoE session at the DSLAM, which is then connected to the BRAS as a PPPoE session. Each PPPoA session is mapped to a corresponding PPPoE session.

Typically, the BRAS is configured to limit PPPoE sessions originating from the same MAC address to protect itself from a DOS attack. This presents a problem for IWF PPPoE sessions because all PPPoE sessions originate from the same MAC address DSLAM. To overcome this issue, the IWF PPPoE tag is inserted at the DSLAM and read by the BRAS to distinguish the IWF PPPoE session from the regular PPPoE session during the PPPoE discovery frames.

For more information about this subject, refer to the DSL Forum Technical Report 101, "Migration to Ethernet-Based DSL Aggregation."

How to Configure PPP-Max-Payload and IWF PPPoE Tag Support

Enabling PPP-Max-Payload and IWF PPPoE Tag Support

To enable the PPP-Max-Payload and IWF PPPoE Tag Support feature, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**]
6. **sessions per-mac iwf limit** *per-mac-limit*
7. **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot* **/subslot/** *port[subinterface]*
8. **pppoe enable [group** *group-name]*
9. **virtual-template** *template-number*
10. **ppp lcp echo mru verify** [**minimum** *value*]
11. **end**
12. **show pppoe session** [**all**| **packets**]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.
Step 5	**tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**] **Example:** `Router(config-bba-group)# tag ppp-max-payload minimum 1200 maximum 3000`	Specifies a range for the ppp-max payload tag value that will be accepted by the BRAS. • Default values are 1492 for the minimum and 1500 for the maximum. • The ppp-max-payload tag value accepted from the client cannot exceed the physical interface value for MTU minus 8.
Step 6	**sessions per-mac iwf limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac iwf limit 200`	Specifies a limit for IWF-specific sessions per MAC address (separate from session limits that are not IWF-specific). • If this command is not entered, the normal MAC-address session limit is applied to IWF sessions. • The *per-mac-limit* argument specifies the allowable number of IWF sessions. The default is 100.
Step 7	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot* **/subslot/** *port[subinterface]* **Example:** `Router(config-bba-group)# interface gigabitethernet 0/0/0`	Enters interface configuration mode for a Gigabit Ethernet interface.
Step 8	**pppoe enable [group** *group-name]* **Example:** `Router(config-if)# pppoe enable group 1`	Enables PPPoE sessions on an Ethernet interface or subinterface.

	Command or Action	Purpose
Step 9	**virtual-template** *template-number* **Example:** `Router(config-if)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.
Step 10	**ppp lcp echo mru verify** [**minimum** *value*] **Example:** `Router(config-if)# ppp lcp echo mru verify minimum 1304`	Verifies the negotiated MRU and adjusts the PPP virtual access interface MTU for troubleshooting purposes. • If the optional **minimum** keyword is entered, the *value* can be from 64 to 1500. • If the verification of minimum MTU succeeds, the PPP connection's interface MTU is set to that value. This reset is useful when you troubleshoot and need to adjust the sessions according to underlying physical network capability. After this command is configured, IP Control Protocol (IPCP) is delayed until verification of the MTU is completed at the LCP.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 12	**show pppoe session** [**all**| **packets**] **Example:** `Router# show pppoe session all`	Verifies the configuration and displays session information. • **all** --Displays output indicating if a session is IWF-specific or if the PPP-Max-Payload tag is in the discovery frame and accepted. • **packets** --Displays packet statistics for the PPPoE session.

Disabling PPP-Max-Payload and IWF PPPoE Tag Support

The **tag ppp-max-payload** command adjusts PPP MTU of the PPPoE session above the default maximum limit of 1492 bytes. But MTU values greater than 1492 can only be supported (with PPPoE) if the underlying Ethernet network supports these larger frames. Not all Ethernet networks support higher values. If your network does not support values higher than the default maximum, you should disable the PPP-Max-Payload and IWF PPPoE Tag Support feature by performing this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **tag ppp-max-payload deny**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters interface configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config-if)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.
Step 4	**tag ppp-max-payload deny** **Example:** `Router(config-bba-group)# tag ppp-max-payload deny`	Disables the processing of the ppp-max-payload tag value higher than the default of 1492 bytes.

Configuration Examples for PPP-Max Payload and IWF PPPoE Tag Support

This section provides a sample configuration showing the PPP-Max-Payload and IWF PPPoE Tag Support feature enabled and a configuration in which the effects of this feature are disabled:

PPP-Max-Payload and IWF PPPoE Tag Support Enabled Example

The following configuration example shows the PPP-Max-Payload and IWF PPPoE Tag Support enabled to accept PPP-Max-Payload tag values from 1492 to 1892, limits the number of sessions per MAC address to 2000 when the IWF is present, and verifies that the PPP session can accept 1500-byte packets in both directions:

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload minimum 1492 maximum 1892
 sessions per-mac limit 1
 sessions per-mac iwf limit 2000
 ppp lcp echo mru verify
!
 interface Virtual-Template 1
!
```

PPP-Max-Payload and IWF PPPoE Tag Support Disabled Example

The following configuration example disables the effect of the **tag ppp-max-payload** command:

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload deny
```

Additional References

The following sections provide references related to the PPP-Max-Payload and IWF PPPoE Tag Support feature.

Related Documents

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* •

Standards

Standard	Title
DSL Forum Technical Report 101	Migration to Ethernet-Based DSL Aggregation

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
Draft RFC document	Accommodating an MTU/MRU Greater than 1492 in PPPoE

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

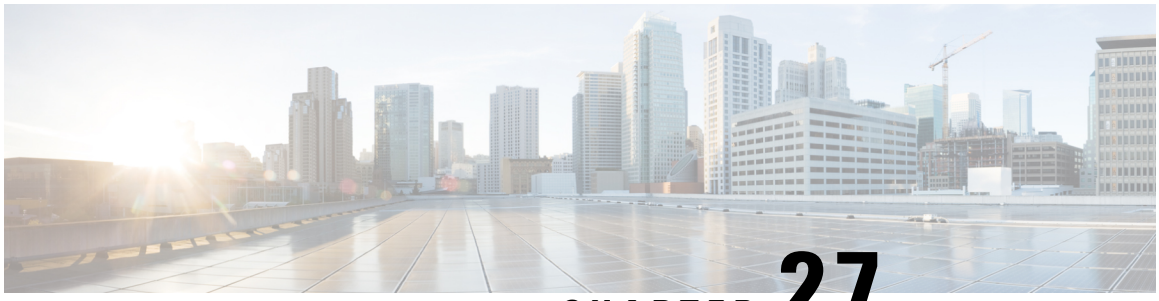
Feature Information for PPP-Max-Payload and IWF PPPoE Tag Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 31: Feature Information for PPP-Max-Payload and IWF PPPoE Tag Support

Feature Name	Releases	Feature Information
PPP-Max Payload and IWF PPPoE Tag Support	Cisco IOS XE Release 2.3	This feature was introduced on Cisco ASR 1000 Series Routers. This feature enables the PPP over Ethernet (PPPoE) component to process the PPP-Max-Payload and Interworking Functionality (IWF) PPPoE tags in the PPPoE discovery frame. The following commands were introduced or modified: **ppp lcp echo mru verify**, **sessions per-mac iwf limit**, **show pppoe session**, **tag ppp-max-payload**.



CHAPTER 27

PPPoE Session Limiting on Inner QinQ VLAN

The PPPoE Session Limiting on Inner QinQ VLAN feature allows a service provider to limit each customer to one PPP over Ethernet (PPPoE) client in use by providing the ability to limit the number of PPPoE over QinQ (IEEE 802.1Q VLAN tunnel) sessions based on the inner VLAN ID configured under a subinterface. This capability eliminates the need to configure large numbers of subinterfaces.

Prerequisites for PPPoE Session Limiting on Inner QinQ VLAN

- PPPoE server functionality must be configured.
- The PPPoE over IEEE 802.1Q VLANs feature must be configured.

Restrictions for PPPoE Session Limiting on Inner QinQ VLAN

- Do not configure the inner VLAN session limit to be greater than the outer session limit.

Information About PPPoE Session Limiting on Inner QinQ VLAN

Benefits of PPPoE Session Limiting on Inner QinQ VLAN

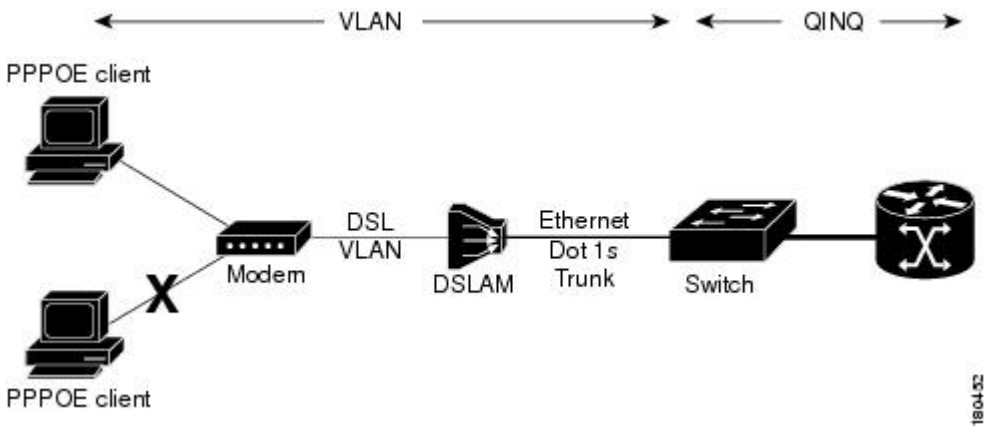
- Facilitates the ability to provision thousands of PPPoE over QinQ sessions having unique inner VLANs using simpler and easier to manage configurations.
- Allows service providers to limit PPPoE sessions based on the QinQ inner VLAN ID.

Feature Design of PPPoE Session Limiting on Inner QinQ VLAN

Prior to the PPPoE Session Limiting on Inner QinQ VLAN feature, PPPoE session limiting required a QinQ subinterface to be configured for each QinQ inner VLAN to be session limited, resulting in configuration requirements that did not scale to large numbers of QinQ VLAN ID pairs. The PPPoE Session Limiting on Inner QinQ VLAN feature adds broadband remote access server (BRAS) capability for configuring a single subinterface for all the unique inner VLAN IDs per outer VLAN while limiting one session per inner VLAN.

The figure below shows a typical implementation of the PPPoE Session Limiting on Inner QinQ VLAN feature.

Figure 25: PPPoE over QinQ Session Limiting



How to Configure PPPoE Session Limiting on Inner QinQ VLAN

Configuring PPPoE Session Limiting on Inner QinQ VLAN

Perform this task to configure PPPoE over QinQ session limiting and allows limiting, which allows you to limit the number of QinQ inner VLAN connections for each customer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **sessions per-vlan limit outer-per-vlan-limit inner inner-per-vlan-limit**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe group 1`	Creates a PPPoE profile and enters the bba-group configuration mode.
Step 4	**sessions per-vlan limit outer-per-vlan-limit inner inner-per-vlan-limit** **Example:** `Router(config-bba-group)# sessions per-vlan-limit 400 inner 1`	Configures inner and outer VLAN limits.
Step 5	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot PPPoE session limiting:

- debug pppoe error
- show pppoe session
- show pppoe summary

Configuration Examples for PPPoE Session Limiting on Inner QinQ VLAN

PPPoE Session Limiting on Inner QinQ VLAN Example

The following example shows how to enable PPPoE over QinQ session limiting on Fast Ethernet interface 1/0/0.1 with outer VLAN ID 10 and a unique inner VLAN ID for each session.

```
Router(config)# bba-group pppoe group1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vlan limit 1000 inner 1
```

```
Router(config)#interface eth1/0/0.1
Router(config-subif)# encapsulation dot1q 10 second-dot1q any
Router(config-subif)# enable group group1
```

Additional References

The following sections provide references related to the PPPoE Session Limiting on Inner QinQ VLAN feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
Broadband access commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
IEEE Standard 802.1Q	Virtual Bridged Local Area Networks

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	*PPP over Ethernet*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

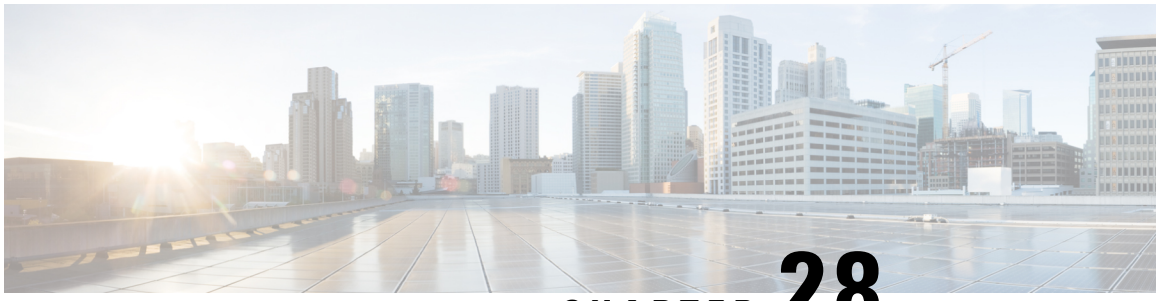
Feature Information for PPPoE Session Limiting on Inner QinQ VLAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 32: Feature Information for PPPoE Session Limiting on Inner QinQ VLAN

Feature Name	Releases	Feature Information
PPPoE Session Limiting on Inner QinQ VLAN	Cisco IOS XE Release 2.1	The PPPoE Session Limiting on Inner QinQ VLAN feature provides the ability to limit the number of PPPoE over QinQ, (IEEE 802.1Q VLAN tunnel) sessions based on the inner VLAN ID configured under a subinterface. In 12.2(31)SB2, this feature was introduced on the Cisco 10000 router. The following command was modified by this feature: **session per-vlan limit**.



CHAPTER 28

PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

The PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature provides a method by which the digital subscriber line access multiplexer (DSLAM) sends the DSL Remote-ID tag in the discovery phase as an identifier for the authentication, authorization, and accounting (AAA) access request on an Fast or Gigabit Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Fast or Gigabit Ethernet instead. This Remote-ID tag is useful for troubleshooting, authentication, and accounting.

Prerequisites for the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

It is recommended that you be familiar with the following documents before configuring this feature:

- RFC 2516: A Method for Transmitting PPP over Ethernet (PPPoE)
- DSL Forum 2004-71: Solution for a Remote-ID in PPPoE Discovery Phase

See the Additional References, on page 315 for more information.

Information About the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Differences Between ATM and Fast or Gigabit Ethernet-Based Broadband Access Networks

Broadband DSLAM and Broadband Remote Access Server (BRAS) vendors need to provide Fast or Gigabit Ethernet-based networks as an alternative to an ATM access network, with a DSLAM bridging the ATM-DSL local loop to the Fast or Gigabit Ethernet-based broadband access network and allowing Fast or Gigabit Ethernet-based connectivity to the BRAS. There is no unique mapping between the subscriber Line-ID tag and the interface in an Fast or Gigabit Ethernet broadband access network, as there is in an ATM-based broadband network, where the ATM VC is associated to a subscriber line. During the authentication phase that initiates the PPP access and AAA accounting requests, the BRAS includes a NAS-Port-ID attribute in RADIUS authentication packets that identifies the DSL for the subscriber

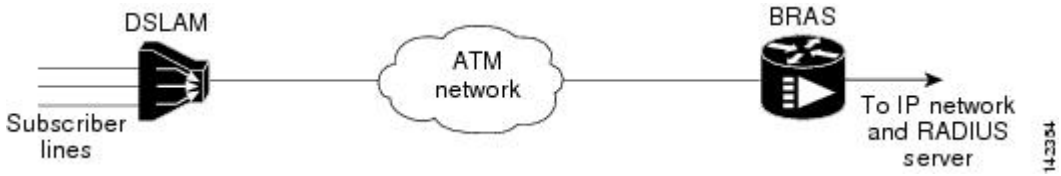
DSL Forum 2004-71 Solution for Remote-ID in PPPoE Discovery Phase

DSL Forum 2004-71 defines a method whereby the DSLAM sends the DSL Remote-ID tag in the PPP over Ethernet (PPPoE) discovery phase to apply the same subscriber mapping capability to Fast or Gigabit Ethernet interfaces that is possible on ATM interfaces. This method adds support for the PPPoE server acting as a BRAS to report the Remote-ID tag as a new vendor specific attribute (VSA) (AAA_AT_REMOTE_ID) in AAA authentication and accounting requests. If the **radius-server attribute 31 remote-id** command is configured on the BRAS, the Remote-ID tag will be sent to a RADIUS server as the Calling Station-ID tag (attribute 31).

Remote-ID Tag in Fast or Gigabit Ethernet-Based Broadband Access Networks

Traditional ATM-based DSL broadband access networks have the topology shown in The figure below.

Figure 26: ATM-Based DSL Broadband Access Network

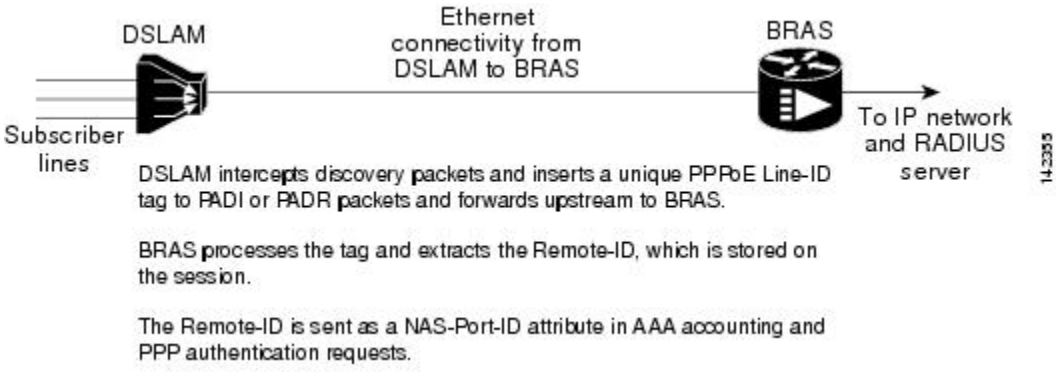


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM virtual circuit (VC) used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-ID tag for use in RADIUS packets.

The simple mapping available from an ATM-based broadband network between the physical line in the DSL local loop to the end user and a virtual circuit (from DSLAM to BRAS) is not available for a Fast or Gigabit Ethernet-based network. To solve this problem, the PPPoE Remote-ID Tag Processing feature uses a PPPoE intermediate agent function on the DSLAM to attach a tag to the PPPoE discovery packets. The BRAS then receives the tagged packet, decodes the tag, and inserts the line identifier into RADIUS packets destined for the RADIUS server.

The DSLAM intercepts PPPoE discovery frames from the client or initiates a discovery frame if the PPPoE Active Discovery (PAD) client is a legacy PPP over ATM (PPPoA) device. The DSLAM inserts a unique Remote-ID tag and DSL sync rate tag using the PPPoE vendor-specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) packets; see the figure below. The DSLAM forwards these packets upstream to the BRAS after the insertion. The tag contains the identification of the DSL line on which the PADI or PADR packet was received, in the access node where the intermediate agent resides.

Figure 27: PPPoE Remote-ID Tag Processing Solution



When the **vendor-tag remote-id service** command is configured in broadband access (BBA) group configuration mode, the BRAS processes the received PPPoE vendor-specific tag in the PADR frame and extracts the Remote-ID tag, which is sent to the remote AAA server as a VSA in all AAA access and accounting requests. When the **radius-server attribute 31 remote-id**global configuration command is also configured on the BRAS, the Remote-ID value is inserted into attribute 31.

Outgoing PAD Offer (PADO) and PAD Session-Confirmation (PADS) packets from the BRAS have the DSLAM-inserted Remote-ID tag. The DSLAM should strip the tag out of PADO and PADS frames. If the DSLAM cannot strip off the tag, the BRAS must remove the tag before sending the frames out. This is accomplished using the **vendor-tag strip** BBA group configuration mode command. If this command is configured under the BBA group, the BRAS strips the incoming Remote-ID tag (and any other vendor tag) off of the outgoing PADO and PADS frames. This action complies with DSL Forum Technical Report 101 .

Benefits of the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

The shift toward Fast or Gigabit Ethernet-based DSLAMs offers the following benefits:

- Ability to use simpler and lower-cost provisioning options for DSL subscribers over a Fast or Gigabit Ethernet-based backhaul network rather than on an ATM-based network.
- Ability to use higher bandwidth connectivity options available from Fast or Gigabit Ethernet that are not possible on ATM.
- Ability to upgrade to next-generation DSLAMs with quality of service (QoS), and support for higher bandwidth, asymmetric dual latency modems such as the ADSL2.

Ability to inject high-bandwidth content such as video in a Fast or Gigabit Ethernet network.

How to Configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Configuring the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement Feature

This task describes how to configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature. When this feature is configured, BRAS will process the incoming PADR frames and send the Remote-ID field of the incoming tag to the RADIUS server as a VSA.

For DSL-Sync-Rate tags, you must enter the **vendor-tag dsl-sync-rate service** command under a BBA group. When this command is entered, the BRAS will process incoming PADR frames and send the DSL-Sync-Rate tags to the RADIUS server as VSAs.

An Access-Accept message is sent by the RADIUS server and vendor-tag attributes sent in the Access-Request message will be present in the Access-Accept message if the RADIUS server echoes it back.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server attribute 31 remote-id**
5. **bba-group pppoe** *group-name*
6. **vendor-tag remote-id service**
7. **vendor-tag dsl-sync-rate service**
8. **nas-port-id format c**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:**	(Optional) Enables the AAA access control model.

	Command or Action	Purpose
	`Router(config)# aaa new-model`	
Step 4	**radius-server attribute 31 remote-id** **Example:** `Router(config)# radius-server attribute 31 remote-id`	(Optional) Sends the Remote-ID tag to the RADIUS server via a new VSA (AAA_AT_REMOTE_ID) and in attribute 31--Calling Station ID.
Step 5	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 6	**vendor-tag remote-id service** **Example:** `Router(config-bba-group)# vendor-tag remote-id service`	Enables the BRAS to process incoming PADR frames and send the Remote-ID field of the incoming tag to the RADIUS server as a VSA.
Step 7	**vendor-tag dsl-sync-rate service** **Example:** `Router(config-bba-group)# vendor-tag dsl-sync-rate service`	Enables the BRAS to process the incoming PADR frames and send the DSL-Sync-Rate tags to the RADIUS server as VSAs.
Step 8	**nas-port-id format c** **Example:** `Router(config-bba-group)# nas-port-id format c`	Specifies a format for broadband subscriber access line identification coding. • The designation of **format c**is specifically designed for a particular coding format. A sample of this format is as follows: NAS_PORT_ID=atm 31/31/7:255.65535 example001/0/31/63/31/127 • This means the subscriber interface type of the BRAS equipment is an ATM interface. The BRAS slot number is 31, and the BRAS subslot number is 31. The BRAS port number is 7. The virtual path identifier (VPI) is 255, and the virtual circuit identifier (VCI) is 65535. The Circuit-ID/Remote-ID tag is example001/0/31/63/31/127.
Step 9	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

Stripping Vendor-Specific Tags

Outgoing PADO and PADS packets will have the DSLAM-inserted Remote-ID and DSL-Sync-Rate tags, and the DSLAM must strip these tags from the packets. If the DSLAM cannot strip the tag, the BRAS must remove it before sending out the packets. This task is accomplished through configuration of the **vendor-tag strip** command in BBA group configuration mode. Note that the **vendor-tag strip** command also removes the Circuit-ID tag.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**vendor-tag strip** **Example:** `Router(config-bba-group)# vendor-tag strip`	Enables the BRAS to strip off incoming vendor-specific tags (including Remote-ID, DSL-Sync-Rate tags, and Circuit-ID) from outgoing PADO and PADS frames.
Step 5	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

Troubleshooting Tips

When you enter the **radius-server attribute 31 remote-id**global configuration command in the PPPoE Agent Remote-ID Tag and DSL Line Characteristics Enhancement feature configuration on the BRAS, you can use the **debug radius** privileged EXEC command to generate a report.

The report includes information about the:

- Incoming access interface
- Location where discovery frames are received
- Details of the sessions being established in PPPoE extended NAS-Port format (format d)

Configuration Examples for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Configuring PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement Example

In the following example, outgoing PADO and PADS packets will retain the incoming Vendor-Specific Circuit-ID tag:

```
Router(config)# radius-server attribute 31 remote-id
!
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag remote-id service
Router(config-bba-group)# vendor-tag dsl-sync-rate service
Router(config-bba-group)# nas-port-id format c
!
Router(config)# interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

Stripping Vendor-Specific Tags Example

In the following example, the BRAS will strip off incoming Vendor-Specific Circuit-ID tags from outgoing PADO and PADS packets:

```
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag strip
Router(config)#interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

Additional References

The following sections provide references related to the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature.

Related Documents

Related Topic	Document Title
Configuring Broadband and DSL	*Cisco IOS XE Broadband and DSL Configuration Guide*
RADIUS attributes	RADIUS Attributes Overview and RADIUS IETF Attributes module
DSL Line-ID tag solution	RFC 4679 - DSL Forum Vendor Specific RADIUS Attributes
Migration to Fast or Gigabit Ethernet-based DSL aggregation	DSL Forum Technical Report 101

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 33: Feature Information for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Feature Name	Releases	Feature Information
PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement	Cisco IOS XE Release 2.1.	The PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature provides a method by which the digital subscriber line access multiplexer (DSLAM) sends the DSL Remote-ID tag in the discovery phase as an identifier for the authentication, authorization, and accounting (AAA) access request on a Fast or Gigabit Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Fast or Gigabit Ethernet instead. This Remote-ID tag is useful for troubleshooting, authentication, and accounting. The following commands were introduced or modified: **radius-server attribute**, **bba-group pppoe group-name**, **vendor-tag remote-id service**, **vendor-tag dsl-sync-rate service**, **nas-port-id format c**.

Glossary

AAA --authentication, authorization, and accounting.

ATM --Asynchronous Transfer Mode.

BBA --broadband access.

BRAS --Broadband Remote Access Server.

DSLAM --digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

PADO --PPPoE Active Discovery Offer.

PADR --PPPoE Active Discovery Request.

PADS --PPPoE Active Discovery Session-Confirmation.

PPPoE --Point-to-Point Protocol over Ethernet.

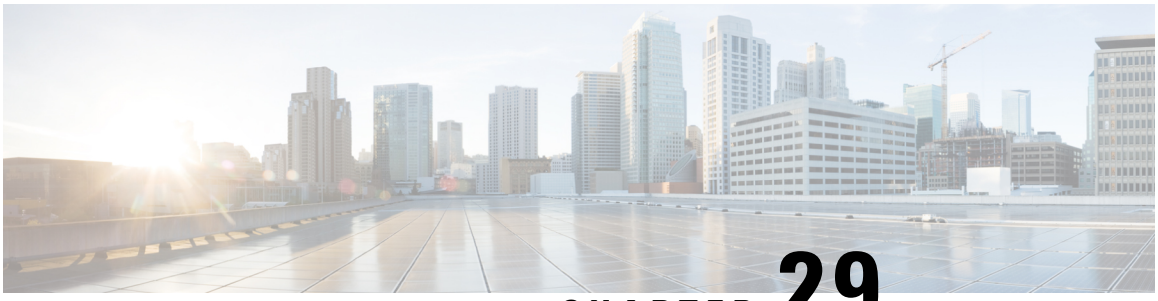
RADIUS --Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

VCI --virtual circuit identifier.

VLAN --virtual local-area network.

VPI --virtual path identifier.

VSA --vendor specific attribute. attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.



CHAPTER 29

Enabling PPPoE Relay Discovery and Service Selection Functionality

The PPPoE Relay feature enables an L2TP access concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP network server (LNS) or tunnel switch (multihop node). The relay functionality of this feature allows the LNS or tunnel switch to advertise the services it offers to the client, thereby providing end-to-end control of services between the LNS and a PPPoE client.

Prerequisites for Enabling PPPoE Relay Discovery and Service Selection Functionality

- You must understand the concepts described in the "Preparing for Broadband Access Aggregation" module.
- PPPoE sessions must be established using the procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module.
- This document assumes you understand how to configure a virtual private dialup network (VPDN) tunnel and a tunnel switch.

Information About Enabling PPPoE Relay Discovery and Service Selection Functionality

L2TP Active Discovery Relay for PPPoE

The PPPoE protocol described in RFC 2516 defines a method for active discovery and service selection of devices in the network by an LAC. A PPPoE client uses these methods to discover an access concentrator in the network, and the access concentrator uses these methods to advertise the services it offers.

The PPPoE Relay feature allows the active discovery and service selection functionality to be offered by the LNS, rather than just by the LAC. The PPPoE Relay feature implements the Network Working Group Internet-Draft titled *L2TP Active Discovery Relay for PPPoE* . The Internet-Draft describes how to relay PPPoE Active Discovery (PAD) and Service Relay Request (SRRQ) messages over an L2TP control channel (the tunnel).

The key benefit of the PPPoE Relay feature is end-to-end control of services between the LNS and a PPPoE client.

Note When the L2TP sessions are created, the traffic does not flow without the appxk9 and ipbasek9 licenses.

How to Enable PPPoE Relay Discovery and Service Selection Functionality

Configuring the LAC and Tunnel Switch for PPPoE Relay

Perform this task to configure the LAC and tunnel switch for PPPoE Relay, which configures a subscriber profile that directs PAD messages to be relayed on an L2TP tunnel. The subscriber profile also will contain an authorization key for the outgoing L2TP tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service relay pppoe vpdn group** *vpdn-group-name*
5. exit

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber profile** *profile-name* **Example:** `Router(config)# subscriber profile profile-1`	Configures the subscriber profile name and enters subscriber profile configuration mode. • *profile-name* --Is referenced from a PPPoE profile configured by the **bba-group pppoe** global configuration command, so that all the PPPoE sessions using the PPPoE profile defined by the **bba-group pppoe**command will be treated according to the defined subscriber profile.
Step 4	**service relay pppoe vpdn group** *vpdn-group-name* **Example:** `Router(config-sss-profile)# service relay pppoe vpdn group Group-A`	Provides PPPoE relay service using a VPDN L2TP tunnel for the relay. The VPDN group name specified is used to obtain outgoing L2TP tunnel information. • See the What to Do Next, on page 321 section for the equivalent RADIUS profile entry.
Step 5	exit **Example:** `Router(config-sss-profile)# exit`	(Optional) Ends the configuration session and returns to privileged EXEC mode.

What to Do Next

Configure the LNS side of the configuration by performing the tasks described in the next section.

Configuring the LNS (or Multihop Node) to Respond to Relayed PAD Messages

On the router that responds to relayed PAD messages, perform this task to configure a PPPoE group and attach it to a VPDN group that accepts dial-in calls for L2TP. The relayed PAD messages will be passed from the VPDN L2TP tunnel and session to the PPPoE broadband group for receiving the PAD responses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *vpdn-group-name*
4. **accept-dialin**
5. **protocol l2tp**

6. **virtual-template** *template-number*
7. **exit**
8. **terminate-from hostname** *host-name*
9. **relay pppoe bba-group** *pppoe-bba-group-name*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *vpdn-group-name* **Example:** `Router(config)# vpdn-group Group-A`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from an LAC and creates an accept-dialin VPDN subgroup.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP tunneling protocol.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-vpdn-req-in)# virtual-template 2`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 7	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.
Step 8	**terminate-from hostname** *host-name* **Example:** `Router(config-vpdn)# terminate-from hostname LAC-1`	Specifies the LAC hostname that will be required when the VPDN tunnel is accepted.

	Command or Action	Purpose
Step 9	**relay pppoe bba-group** *pppoe-bba-group-name* **Example:** `Router(config-vpdn)# relay pppoe bba-group group-2`	Specifies the PPPoE BBA group that will respond to the PAD messages. • The PPPoE BBA group name is defined with the **bba-group pppoe** *group-name* global configuration command.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits to global configuration mode.

Monitoring PPPoE Relay

Perform this task to monitor PPPoE Relay.

SUMMARY STEPS

1. **enable**
2. **show pppoe session**
3. **show pppoe relay context all**
4. **clear pppoe relay context**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pppoe session**

Displays information about currently active PPPoE sessions.

Example:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                     VA-st
     26     19  0001.96da.a2c0  Et0/0.1                  5  N/A RELFWD
                000c.8670.1006  VLAN:3434
```

Step 3 **show pppoe relay context all**

Displays the PPPoE relay context created for relaying PAD messages.

Example:

```
Router# show pppoe relay context all
Total PPPoE relay contexts 1
UID    ID     Subscriber-profile      State
25     18     cisco.com                 RELAYED
```

Example:

Step 4 **clear pppoe relay context**

This command clears the PPPoE relay context created for relaying PAD messages.

Example:

```
Router(config)# clear pppoe relay context
```

Troubleshooting Tips

Use the following commands in privileged EXEC mode to help you troubleshoot the PPPoE Relay feature:

- **debug ppp forwarding**
- **debug ppp negotiation**
- **debug pppoe events**
- **debug pppoe packets**
- **debug vpdn l2x-events**
- **debug vpdn l2x-packets**

Configuration Examples for Enabling PPPoE Relay Discovery and Service Selection Functionality

PPPoE Relay on LAC Configuration Example

The following is an example of a standard LAC configuration with the commands to enable PPPoE relay added:

```
hostname User2
!
username User1 password 0 field
username User2 password 0 field
username user-group password 0 field
username User5 password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
```

```
username User3-lns-domain password 0 field
!
ip domain-name cisco.com
!
vpdn enable
vpdn source-ip 10.0.195.151
!
vpdn-group User2-vpdn-group-domain
 request-dialin
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.133
 local name User2-lac-domain
!
!
interface Loopback123
 ip address 10.22.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.195.151 255.255.255.0
 no keepalive
 half-duplex
 pppoe enable group group-1
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback123
 ppp authentication chap
 ppp chap hostname User2-lac-domain
!
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
subscriber profile Profile1
 service relay pppoe vpdn group User2-vpdn-group-domain
!
bba-group pppoe group-1
 virtual-template 1
 service profile Profile1
!
```

Basic LNS Configured for PPPoE Relay Example

The following example shows the basic configuration for an LNS with commands added for PPPoE relay:

```
hostname User5
!
!
username User5 password 0 field
username user-group password 0 field
username User1 password 0 field
username User2 password 0 field
username User3 password 0 field
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 field
username mysgbpgroup password 0 cisco
username User3-lns-domain password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
```

```
username User5-mh password 0 field
username User1@domain.net password 0 field
ip subnet-zero
!
!
ip domain-name cisco.com
!
vpdn enable
vpdn multihop
vpdn source-ip 10.0.195.133
!
vpdn-group 1
 request-dialin
  protocol l2tp
!
vpdn-group 2
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
!
vpdn-group User5-mh
 request-dialin
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.143
 local name User5-mh
!
vpdn-group User3-vpdn-group-domain
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname User2-lac-domain
 local name User3-lns-domain
 relay pppoe group group-1
!
!
interface Loopback0
 no ip address
!
!
interface Loopback123
 ip address 10.23.3.2 255.255.255.0
!
!
interface FastEthernet0/0
 ip address 10.0.195.133 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
!
!
interface Virtual-Template2
 mtu 1492
 ip unnumbered Loopback123
 ip access-group virtual-access3#234 in
 ppp mtu adaptive
 ppp authentication chap
 ppp chap hostname User3-lns-domain
!
!
ip default-gateway 10.0.195.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
```

```
!
bba-group pppoe group-1
 virtual-template 2
!
```

Tunnel Switch (or Multihop Node) Configured to Respond to PAD Messages Example

The following is an example of a standard tunnel switch configuration with the commands to enable response to PPPoE relay messages added:

```
hostname User3
!
!
username User1 password 0 room1
username User2 password 0 room1
username User3 password 0 room1
username User1@domain.net password 0 room1
username User3-lns-dnis password 0 cisco
username User3-lns-domain password 0 room1
username User2-lac-dnis password 0 cisco
username User2-lac-domain password 0 room1
username User5 password 0 room1
username User5-mh password 0 room1
username user-group password 0 room1
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 room1
username mysgbpgroup password 0 cisco
username User1-client-domain@cisco.net password 0 room1
username User4-lns-domain password 0 room1
!
ip domain-name cisco.com
!
vpdn enable
!
vpdn-group User3-mh
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname User5-mh
 relay pppoe bba-group group-1
!
interface Loopback0
 ip address 10.4.4.2 255.255.255.0
!
interface Loopback1
 ip address 10.3.2.2 255.255.255.0
!
interface Ethernet2/0
 ip address 10.0.195.143 255.255.0.0
 half-duplex
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback0
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
```

```
 ppp chap hostname User3-lns-domain
!
ip default-gateway 10.0.195.1
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
bba-group pppoe group-1
 virtual-template 1
!
```

Tunnel Switch Configured to Relay PAD Messages Example

The following partial example shows a configuration that allows the tunnel switch to relay PAD messages:

```
subscriber profile profile-1
! Configure profile for PPPoE Relay
 service relay pppoe vpdn group Example1.net
.
.
.
vpdn-group Example2.net
! Configure L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from host Host1
 relay pppoe bba-group group-1
.
.
.
vpdn-group Example1.net
! Configure L2TP tunnel for PPPoE Relay
 request-dialin
  protocol l2tp
.
.
.
 initiate-to ip 10.17.1.3
.
.
.
! PPPoE-group configured for relay
bba-group pppoe group-1
.
.
.
service profile profile-1
```

RADIUS Subscriber Profile Entry for the LAC Example

The following example shows how to enter Subscriber Service Switch subscriber service attributes in a AAA RADIUS server profile.

```
profile-1 = profile-name.
.
.
```

Cisco:Cisco-Avpair = "sss:sss-service=relay-pppoe"

The following is an example of a typical RADIUS subscriber profile entry for an LAC:

```
cisco.com Password = "password"
    Cisco:Cisco-Avpair = "sss:sss-service=relay-pppoe",
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Tunnel-Assignment-Id = assignment-id
```

RADIUS VPDN Group User Profile Entry for the LNS Example

The following example shows how to enter the VPDN group attributes in a AAA RADIUS server profile.

```
profile-1 = profile-name.
.
.
   Cisco:Cisco-Avpair = "vpdn:relay-pppoe-bba-group=group-name
```

The following is an example of a typical RADIUS subscriber profile entry for an LNS:

```
cisco.com Password = "password"
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Cisco:Cisco-Avpair = "vpdn:relay-pppoe-bba-group=group-name"
    Tunnel-Assignment-Id = assignment-id
```

Additional References

The following sections provide referenced related to the PPPoE Relay feature.

Related Documents

Related Topic	Document Title
VPDN tunnels	*Cisco IOS XE Dial Technologies Configuration Guide*
VPDN tunnel commands	*Cisco IOS XE Dial Technologies Configuration Guide*
Tunnel switching	L2TP Tunnel Switching feature module
PPPoE broadband groups	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
PPPoE broadband commands	*Cisco IOS XE Broadband Access Aggregation and DSL Command Reference*

Related Topic	Document Title
Broadband access aggregation concepts	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
Tasks for preparing for broadband access aggregation	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2516	*Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 3817	• *L2TP Active Discovery Relay for PPPoE* • Network Working Group Internet-Draft, *L2TP Active Discovery Relay for PPPoE* , which can be seen at http://tools.ietf.org/html/draft-dasilva-l2tp-relaysvc-06

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

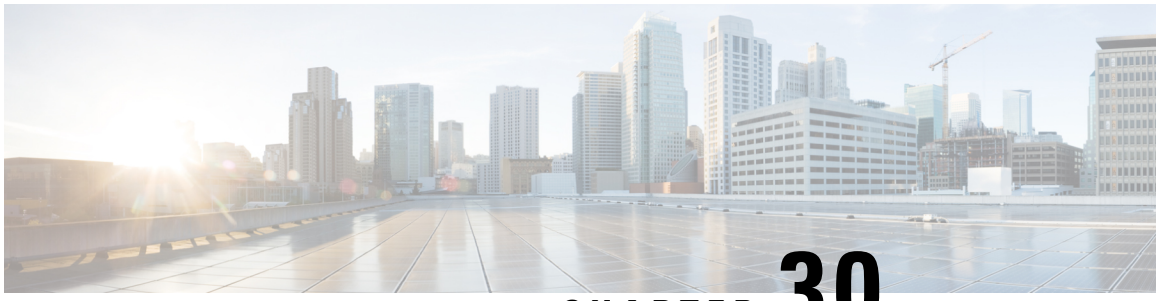
Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 34: Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

Feature Name	Releases	Feature Configuration Information
PPPoE Relay	Cisco IOS XE Release 2.1	The PPPoE Relay feature enables an L2TP access concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP network server (LNS) or tunnel switch (multihop node). This feature was integrated into Cisco IOS XE Release 2.1.
PPPoE Service Selection	Cisco IOS XE Release 2.4	This feature was integrated into Cisco IOS XE Release 2.4.



CHAPTER 30

Configuring Cisco Subscriber Service Switch Policies

The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. The primary focus of the Subscriber Service Switch is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy manages tunneling of PPP in a policy-based bridging fashion.

Prerequisites for Configuring a Subscriber Service Switch Policy

- Before configuring a Subscriber Service Switch policy, you must understand the concepts presented in the "Understanding Broadband Access Aggregation" module.
- Before configuring a Subscriber Service Switch policy, you must perform the PPP over Ethernet (PPPoE) configuration procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module or perform the PPP over ATM (PPPoA) configuration procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions" module.

Restrictions for Configuring a Subscriber Service Switch Policy

The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. The Subscriber Server Switch provides the infrastructure for any protocol to plug into; however, the initial implementation provides switching PPP over Ethernet and

PPP over ATM session to a Layer 2 Tunneling Protocol (L2TP) device such as an L2TP access concentrator (LAC) switch, and switching L2TP sessions to an L2TP tunnel switch only.

Information About the Subscriber Service Switch

The Subscriber Service Switch was developed in response to a need by Internet service providers (ISPs) for increased scalability and extensibility for remote access service selection and Layer 2 subscriber policy management. This Layer 2 subscriber policy is needed to manage tunneling of PPP in a policy-based bridging fashion.

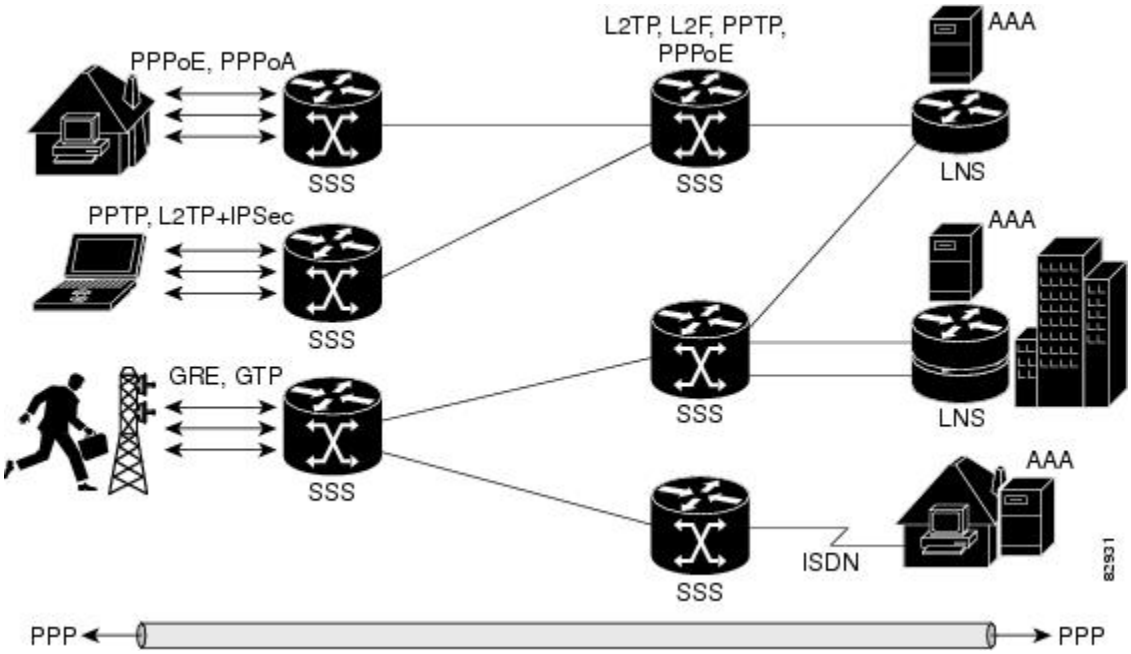
Benefits of the Subscriber Service Switch

The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. In the past, remote access service selection was largely determined by the telephone number dialed or the PPP username and password entered during a PPP authentication cycle. However, broadband, cable, Virtual Private Network (VPN), and wireless access methods have created an environment where PPP sessions may be tunneled over a variety of protocols and media. The multitude of protocols, management domains, network infrastructure, and variety of services has created a complex environment for directing a subscriber to a given service or application. The problem is further complicated by the much greater density of total PPP sessions that can be transported over shared media versus traditional point-to-point links. The Subscriber Service Switch can provide a flexible and extensible decision point linking an incoming subscriber (typically a PPP session over some physical or virtual link) to another tunneled link or local termination for Layer 3 processing.

The Subscriber Service Switch is also scalable in situations where a subscriber's Layer 2 service is switched across virtual links. Examples include switching among PPPoA, PPPoE, L2TP, Layer 2 Forwarding Protocol (L2F), Point-to-Point Tunneling Protocol (PPTP), generic routing encapsulation (GRE), and General Packet Radio Service (GPRS) Tunneling Protocol (GTP wireless data standard).

The figure below shows how the Subscriber Service Switch provides its own centralized switching path that bypasses the virtual-access-based switching available earlier. In the figure below, the Subscriber Service Switch is switching data traffic from personal computers in a home and corporate office and from a wireless user.

Figure 28: Basic Subscriber Service Switch Operation



Protocols that register with the Subscriber Service Switch application programming interface (API) can take advantage of this switching path. Bypassing the virtual access interface in this manner helps the Cisco IOS XE software to scale to the increased number of sessions that the market demands. The Subscriber Service Switch also improves network performance. For example, benchmark testing indicates that performance of L2TP multihop tasks occurs twice as fast in networks with the Subscriber Service Switch as in networks without it.

Backward Compatibility of Subscriber Service Switch Policies

All of the existing virtual private dialup network (VPDN), Multichassis Multilink PPP (MMLP), and local termination policies and configurations are maintained in the implementation of the Subscriber Service Switch; however, default policies may be overridden by the following configurations or events:

- Resource Manager (RM) VPDN authorization is attempted before VPDN authorization.
- VPDN authorization is attempted before Stack Group Forwarding (SGF) MMLP.
- VPDN service authorization is attempted only when the **vpdn enable** command is configured.
- RM VPDN service authorization is attempted only if RM is enabled.
- SGF authorization is attempted only when the **sgbp member** command is configured and one or both of the following service keys are available from the subscriber: unauthenticated PPP name and endpoint discriminator.
- The **dnis** and **domain** service keys, in that order, are used to authorize VPDN service, provided that VPDN service is enabled.
- An unauthenticated PPP name is always reduced to a domain name by taking all characters from the right of the PPP name up to a configurable delimiter character (default is the @ character). Only the domain portion is used to locate a service.

- If the **vpdn authen-before-forward** command is configured as a global configuration command, the authenticated PPP name is used to authorize VPDN service.
- The **vpdn-group** command can define four configurations:
- Authorization for VPDN call termination (using the *accept-dialin* and **accept-dialout** keywords).
- Authorization for VPDN subscriber service (using the **request-dialin** and **request-dialout** keywords).
- A directive to collect further service keys and reauthorize (using the **authen-before-forward** keyword).
- A tunnel configuration.

The Subscriber Service Switch adds a general configuration framework to replace the first three aspects of a VPDN group.

- If VPDN and SGF services either are not configured or cannot be authorized, local PPP termination service is selected. Further PPP authorization is still required to complete local termination.
- A two-phase authorization scheme is enabled by the **vpn domain authorization** command. An NAS-Port-ID (NAS port identifier) key is used to locate the first service record, which contains a restricted set of values for the domain substring of the unauthenticated PPP name. This filtered service key then locates the final service. Cisco refers to this scheme as domain preauthorization.
- Domain preauthorization will occur only when the **NAS-Port-ID** key is available.
- When domain preauthorization is enabled, both authenticated and unauthenticated domain names are checked for restrictions.
- It is possible to associate a fixed service with an ATM permanent virtual circuit (PVC), thus affecting any subscribers carried by the PVC. The **vpn service** command, in ATM VC or VC class configuration mode, and the associated key make up the generic service key.
- When the generic service key is available, it will be used for authorization instead of the unauthenticated domain name.
- If either the **vpdn authen-before-forward** or **per vpdn-group authen-before-forward** command is configured, the authenticated username is required and will be used to authorize VPDN service.
- To determine whether the **authen-before-forward** command is configured in a VPDN group (using the **vpdn-group** command), an unauthenticated username or the generic service key is required as the initial-want key set.
- When the global **vpdn authen-before-forward** command is not configured, the generic service key, if one is available, is used to determine whether the **authen-before-forward** function is configured in the VPDN group (using the **vpdn-group** command). If the generic service key is not available, the unauthenticated username will be used.
- If an accounting-enabled key is available, the unauthenticated username is required.
- VPDN multihop is allowed only when VPDN multihop is enabled.
- SGF on the L2TP network server (LNS) is allowed only when VPDN multihop is enabled on the LNS.
- Forwarding of SGF calls on the LAC is allowed only if VPDN multihop is enabled on the LAC.
- SGF-to-SGF multihop is not allowed.

- When PPP forwarding is configured, both Multilink PPP (MLP) and non-MLP calls are forwarded to the winner of the Stack Group Bidding Protocol (SGBP) bid.
- Authentication is always required for forwarded Packet Data Serving Node (PDSN) calls.
- When the **directed-request** function is enabled and activated using the **ip host** command, VPDN service authorization occurs only when the **vpdn authorize directed-request** command is used.
- Fixed legacy policy is still maintained for RM.

Debug Commands Available for Subscriber Service Switch

The Subscriber Service Switch feature introduces five new EXEC mode **debug** commands to enable diagnostic output about Subscriber Service Switch call operation, as follows:

- **debug sss aaa authorization event** --Displays messages about AAA authorization events that are part of normal call establishment.
- **debug sss aaa authorization fsm** --Displays messages about AAA authorization state changes.
- **debug sss error** --Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
- **debug sss event** --Displays diagnostic information about Subscriber Service Switch call setup events.
- **debug sss fsm** --Displays diagnostic information about the Subscriber Service Switch call setup state.

The following EXEC mode debug commands already exist:

- **debug redundancy** - This command is available on platforms that support redundancy.
- **debug sss elog** --Collects SSS performance event data.
- **debug sss feature** --Enables debug for SSS feature events
- **debug sss packet** --Enables packet level event and information debugging for the Subscriber Service Switch.
- **debug sss policy** --Enables debug for SSS policy module events.
- **debug sss service** --Enables debug for service manager event.

These commands were designed to be used with Cisco IOS XE **debug** commands that exist for troubleshooting PPP and other Layer 2 call operations. The table below lists some of these **debug** commands.

Table 35: Additional Debugging Commands for Troubleshooting the Subscriber Service Switch

Command	Purpose
debug ppp negotiation	Allows you to check that a client is passing PPP negotiation information.
debug pppoe errors	Displays PPPoE error messages.
debug pppoe events	Displays protocol event information.
debug vpdn call events	Enables VPDN call event debugging.

Command	Purpose
debug vpdn call fsm	Enables VPDN call setup state debugging.
debug vpdn elog	Enables VPDN performance event data collection.
debug vpdn events	Displays PPTP tunnel event change information.
debug vpdn 12x-data	Enables L2F and L2TP event and data debugging.
debug vpdn l2x-errors	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.
debug vpdn l2x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn 12x-packets	Enables L2F and L2TP packet level debugging.
debug vpdn errors	Displays PPTP protocol error messages.
debug vpdn message	Enables VPDN inter processing message debugging.
debug vpdn packet	Enables VPDN packet level debugging.
debug vpdn scalability	Enables VPDN scalability debugging.
debug vpdn sss errors	Displays diagnostic information about errors that may occur during VPDN Subscriber Service Switch call setup.
debug vpdn sss events	Displays diagnostic information about VPDN Subscriber Service Switch call setup events.

Note The **debug** commands are intended only for troubleshooting purposes, because the volume of output generated by the software can result in severe performance degradation on the router.

How to Configure a Subscriber Service Switch Policy

The Subscriber Service Switch architecture is transparent, and existing PPP, VPDN, PPPoE, PPPoA, and authentication, authorization, and accounting (AAA) call configurations will continue to work in this environment. You can, however, enable Subscriber Service Switch preauthorization and Subscriber Service Switch type authorization. You may also find it helpful to verify Subscriber Service Switch call operation.

Enabling Domain Preauthorization on a NAS

Perform the following task to enable the NAS to perform domain authorization before tunneling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. vpdn authorize domain

4. **exit**
5. Router# show running-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	vpdn authorize domain **Example:** `Router(config)# vpdn authorize domain`	Enables domain preauthorization on an Network Access Server (NAS).
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	Router# show running-config **Example:** `show running-config`	Displays the configuration so you can check that you successfully enabled domain preauthorization.

What to Do Next

Create a RADIUS user profile for domain preauthorization. See the next section for more information.

Creating a RADIUS User Profile for Domain Preauthorization

The table below contains the attributes needed to enable domain preauthorization in a RADIUS user file. Refer to the Cisco IOS XE Security Configuration Guide for information about creating a RADIUS user profile.

Table 36: Attributes for the RADIUS User Profile for Domain Preauthorization

RADIUS Entry	Purpose
nas-port: *ip-address:slot/subslot/port/vpi.vci*	Configures the NAS port username for domain preauthorization. • *ip-address* **:** --Management IP address of the node switch processor (NSP). • *slot* **/** *subslot* **/** *port* --Specifies the ATM interface. • *vpi* **.** *vci* --Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.
Password= "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service type as outbound.
Cisco-AVpair= "vpdn:vpn-domain-list= *domain1*, domain2,..."	Specifies the domains accessible to the user. • *domain* --Domain to configure as accessible to the user.

Enabling a Subscriber Service Switch Preauthorization

When Subscriber Service Switch preauthorization is enabled on an LAC, local configurations for session limit per VC and per VLAN are overwritten by the per-NAS-port session limit downloaded from the server. Perform this task to enable preauthorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id**[*aaa-method-list*]
4. **show sss session [all]**
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber access** {**pppoe**	**pppoa**} **pre-authorize nas-port-id**[*aaa-method-list*]	Enables Subscriber Service Switch preauthorization.

	Command or Action	Purpose
	Example: **Example:** `Router(config)# subscriber access pppoe pre-authorize nas-port-id mlist-llid` **Example:**	**Note** The LACs maintain a current session number per NAS port. As a new session request comes in, the LAC makes a preauthorization request to AAA to get the session limit, and compares it with the number of sessions currently on that NAS port. This command ensures that session limit querying is only enabled for PPPoE-type calls, not for any other call types.
Step 4	**show sss session [all]** **Example:** `Router(config)# show sss session all`	Displays the Subscriber Service Switch session status.
Step 5	exit **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode.

What to Do Next

Information about troubleshooting a network running the Subscriber Service Switch can be found in the next section.

Troubleshooting the Subscriber Service Switch

Perform this task to troubleshoot the Subscriber Service Switch. Examples of normal and failure operations can be found in the Troubleshooting the Subscriber Service Switch Examples, on page 346. Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Perform the following task to troubleshoot a network running the Subscriber Service Switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Use Telnet to access a router port and repeat Steps 2 and 3.
5. **terminal monitor**
6. **exit**
7. **debug sss** *command-option*
8. **configure terminal**
9. **no terminal monitor**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no logging console** **Example:** `Router(config)# no logging console`	Disables all logging to the console terminal. • To reenable logging to the console, use the **logging console** command.
Step 4	Use Telnet to access a router port and repeat Steps 2 and 3.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 5	**terminal monitor** **Example:** `Router(config)# terminal monitor`	Enables logging output on the virtual terminal.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 7	**debug sss** *command-option* **Example:** `Router# debug sss error`	Enables the **debug** command. **Note** You can enter more than one **debug** command.
Step 8	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 9	**no terminal monitor** **Example:** `Router(config)# no terminal monitor`	Disables logging on the virtual terminal.
Step 10	**exit** **Example:**	Exits to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config)# exit`	

Configuration Examples for Configuring a Subscriber Service Switch Policy

LAC Domain Authorization Example

The following example shows the configuration necessary for the LAC to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Domain Preauthorization RADIUS User Profile Example

The following example shows a typical domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
 check_items= {
 2=cisco
 }
 reply_attributes= {
 9,1="vpdn:vpn-domain-list=example1.com,example2.com"
 6=5
 }
 }
 }
```

Subscriber Service Switch Preauthorization Example

The following partial example signals the Subscriber Service Switch to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to all sessions with a PPPoE access type.

```
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
```

```
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist-llid
!
```

Verify Subscriber Service Switch Call Operation Example

The following example command output from the **show sss session all** command provides an extensive report of Subscriber Service Switch session activity. Each section shows the unique identifier for each session, which can be used to correlate that particular session with the session information retrieved from other **show** commands or **debug** command traces. See the following **show vpdn session** command output for an example of this unique ID correlation.

```
Router# show sss session all
Current SSS Information: Total sessions 9
SSS session handle is 40000013, state is connected, service is VPDN
Unique ID is 9
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:49
Root SIP Handle is DF000010, PID is 49
AAA unique ID is 10
Current SIP options are Req Fwding/Req Fwde
SSS session handle is B0000017, state is connected, service is VPDN
Unique ID is 10
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:05
Root SIP Handle is B9000015, PID is 49
AAA unique ID is 11
Current SIP options are Req Fwding/Req Fwded
SSS session handle is D6000019, state is connected, service is VPDN
Unique ID is 11
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:13
Root SIP Handle is D0000016, PID is 49
AAA unique ID is 12
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 8C000003, state is connected, service is VPDN
Unique ID is 3
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user3@example.com
Last Changed 2d21h
Root SIP Handle is D3000002, PID is 49
AAA unique ID is 3
Current SIP options are Req Fwding/Req Fwded
SSS session handle is BE00000B, state is connected, service is Local Term
Unique ID is 6
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user1
Last Changed 00:03:56
Root SIP Handle is A9000009, PID is 49
AAA unique ID is 7
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DC00000D, state is connected, service is Local Term
Unique ID is 7
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user2
Last Changed 00:03:57
Root SIP Handle is 2C00000A, PID is 49
```

```
AAA unique ID is 8
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DB000011, state is connected, service is VPDN
Unique ID is 8
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:58
Root SIP Handle is 1000000F, PID is 49
AAA unique ID is 9
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 3F000007, state is connected, service is Local Term
Unique ID is 2
SIP subscriber access type(s) are PPP
Identifier is user1
Last Changed 00:05:30
Root SIP Handle is 8A000009, PID is 92
AAA unique ID is 1
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 97000005, state is connected, service is VPDN
Unique ID is 4
SIP subscriber access type(s) are PPP
Identifier is nobody2@example.com
Last Changed 00:07:16
Root SIP Handle is 32000000, PID is 92
AAA unique ID is 5
Current SIP options are Req Fwding/Req Fwded
```

Correlating the Unique ID in show vpdn session Command Output

The following partial sample output from the **show vpdn session** command provides extensive reports on call activity for all L2TP, L2F, and PPPoE sessions, and identifies the unique ID for each session.

```
Router# show vpdn session all
L2TP Session Information Total tunnels 1 sessions 4
Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody3@example.com
    Interface
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8
Session id 6 is up, tunnel id 13695
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody3@example.com
    Interface
```

```
  Remote session id is 693, remote tunnel id 58582
UDP checksums are disabled
SSS switching enabled
No FS cached header information available
Sequencing is off
Unique ID is 9
```

Troubleshooting the Subscriber Service Switch Examples

This section provides the following debugging session examples for a network running the Subscriber Service Switch:

Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Troubleshooting the Subscriber Service Switch Operation Example

The following example shows the **debug** commands used and sample output for debugging Subscriber Service Switch operation:

```
Router# debug sss event
Router# debug sss error
Router# debug sss state
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on
*Mar  4 21:33:18.248: SSS INFO: Element type is Access-Type, long value is 3
*Mar  4 21:33:18.248: SSS INFO: Element type is Switch-Id, long value is -1509949436
*Mar  4 21:33:18.248: SSS INFO: Element type is Nasport, ptr value is 6396882C
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-ACCT_ENBL, long value is 1
*Mar  4 21:33:18.248: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:18.248: SSS PM [uid:7]: Need the following key: Unauth-User
*Mar  4 21:33:18.248: SSS PM [uid:7]: Received Service Request
*Mar  4 21:33:18.248: SSS PM [uid:7]: Event <need keys>, State: initial-req to
need-init-keys
*Mar  4 21:33:18.248: SSS PM [uid:7]: Policy reply - Need more keys
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Got reply Need-More-Keys from PM
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event policy-or-mgr-more-keys, state changed from
wait-for-auth to wait-for-req
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling More-Keys event
*Mar  4 21:33:20.256: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Mar  4 21:33:20.256: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:20.256: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:20.256: SSS INFO: Element type is Access-Type, long value is 0
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:20.256: SSS PM [uid:7]: Received More Initial Keys
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <rcvd keys>, State: need-init-keys to
check-auth-needed
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling Authorization Check
```

```
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <send auth>, State: check-auth-needed to
authorizing
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling AAA service Authorization
*Mar  4 21:33:20.256: SSS PM [uid:7]: Sending authorization request for 'example.com'
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Event <make request>, state changed from idle

to authorizing
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Authorizing key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:AAA request sent for key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Received an AAA pass
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <found service>, state changed from
authorizing to complete
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Found service info for key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <free request>, state changed from
complete to terminal
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Free request
*Mar  4 21:33:20.264: SSS PM [uid:7]: Event <found>, State: authorizing to end
*Mar  4 21:33:20.264: SSS PM [uid:7]: Handling Service Direction
*Mar  4 21:33:20.264: SSS PM [uid:7]: Policy reply - Forwarding
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Got reply Forwarding from PM
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Event policy-start-service-fsp, state changed from
wait-for-auth to wait-for-service
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Handling Connect-Forwarding-Service event
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Event service-fsp-connected, state changed from
wait-for-service to connected
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Handling Forwarding-Service-Connected event
```

Troubleshooting the Subscriber Service Switch on the LAC--Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LAC:

```
Router# debug sss event
Router# debug sss error
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm
Router# debug pppoe events
Router# debug pppoe errors
Router# debug ppp negotiation
Router# debug vpdn l2x-events
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn call events
Router# debug vpdn call fsm
Router# debug vpdn events
Router# debug vpdn errors
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE protocol errors debugging is on
PPP:
  PPP protocol negotiation debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
```

```
  VPDN call event debugging is on
  VPDN call FSM debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
*Nov 15 12:23:52.523: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:23:52.523: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE : encap string prepared
*Nov 15 12:23:52.527: [13]PPPoE 10: Access IE handle allocated
*Nov 15 12:23:52.527: [13]PPPoE 10: pppoe SSS switch updated
*Nov 15 12:23:52.527: [13]PPPoE 10: Service request sent to SSS
*Nov 15 12:23:52.527: [13]PPPoE 10: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:23:52.547: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:23:52.547: SSS INFO: Element type is Switch-Id, long value is 2130706444
*Nov 15 12:23:52.547: SSS INFO: Element type is Nasport, ptr value is 63C07288
*Nov 15 12:23:52.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:52.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:52.547: SSS PM [uid:13]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:23:52.547: SSS PM [uid:13]: Received Service Request
*Nov 15 12:23:52.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy requires 'Unauth-User' key
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy reply - Need more keys
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Got reply Need-More-Keys from PM
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling More-Keys event
*Nov 15 12:23:52.547: [13]PPPoE 10: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:23:52.547: [13]PPPoE 10: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.547: ppp13 PPP: Using default call direction
*Nov 15 12:23:52.547: ppp13 PPP: Treating connection as a dedicated line
*Nov 15 12:23:52.547: ppp13 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:23:52.547: ppp13 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:23:52.547: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.547: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:52.547: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:52.547: [13]PPPoE 10: State START_PPP    Event DYN_BIND
*Nov 15 12:23:52.547: [13]PPPoE 10: data path set to PPP
*Nov 15 12:23:52.571: ppp13 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:    MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:52.571: ppp13 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:    MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:54.543: ppp13 LCP: TIMEout: State ACKsent
*Nov 15 12:23:54.543: ppp13 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: State is Open
*Nov 15 12:23:54.543: ppp13 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:23:54.543: ppp13 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:23:54.547: ppp13 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
*Nov 15 12:23:54.547: ppp13 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:23:54.547: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
```

```
*Nov 15 12:23:54.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:54.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:54.547: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:23:54.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:54.547: SSS PM [uid:13]: Received More Keys
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling AAA service Authorization
*Nov 15 12:23:54.547: SSS PM [uid:13]: Sending authorization request for 'example.com'
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Authorizing key example.com
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:AAA request sent for key example.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Received an AAA pass
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Found service info for key example.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Free request
*Nov 15 12:23:54.551: SSS PM [uid:13]: Handling Service Direction
*Nov 15 12:23:54.551: SSS PM [uid:13]: Policy reply - Forwarding
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Got reply Forwarding from PM
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Handling Connect-Service event
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Event connect req, state changed from idle
to connecting
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Requesting connection
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Call request sent
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Event client connect, state changed from
idle to connecting
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Initiating compulsory connection to
192.168.8.2
*Nov 15 12:23:54.551:   Tnl/Sn61510/7 L2TP: Session FS enabled
*Nov 15 12:23:54.551:   Tnl/Sn61510/7 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:23:54.551: uid:13  Tnl/Sn61510/7 L2TP: Create session
*Nov 15 12:23:54.551: uid:13  Tnl/Sn61510/7 L2TP: O ICRQ to rp1 9264/0
*Nov 15 12:23:54.551: [13]PPPoE 10: Access IE nas port called
*Nov 15 12:23:54.555:   Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.555: uid:13  Tnl/Sn61510/7 L2TP: Session state change from
wait-for-tunnel to wait-reply
*Nov 15 12:23:54.555: [13]PPPoE 10: State LCP_NEGO    Event PPP_FWDING
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: O ICCN to rp1 9264/13586
*Nov 15 12:23:54.559:   Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: Session state change from
wait-reply to established
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: VPDN session up
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Event peer connected, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Succeed to forward nobody@example.com
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: accounting start sent
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Connection succeeded
*Nov 15 12:23:54.559: SSS MGR [uid:13]: Handling Service-Connected event
*Nov 15 12:23:54.559: ppp13 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:23:54.559: [13]PPPoE 10: State LCP_NEGO    Event PPP_FWDED
*Nov 15 12:23:54.563: [13]PPPoE 10: data path set to SSS Switch
*Nov 15 12:23:54.563: [13]PPPoE 10: Connected Forwarded
```

Troubleshooting the Subscriber Service Switch on the LAC--Authorization Failure Example

The following is sample output indicating call failure due to authorization failure:

```
*Nov 15 12:37:24.535: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:37:24.535: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE : encap string prepared
*Nov 15 12:37:24.539: [18]PPPoE 15: Access IE handle allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: pppoe SSS switch updated
*Nov 15 12:37:24.539: PPPoE 15: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA unique ID allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: No AAA accounting method list
*Nov 15 12:37:24.539: [18]PPPoE 15: Service request sent to SSS
*Nov 15 12:37:24.539: [18]PPPoE 15: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:37:24.559: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:37:24.559: SSS INFO: Element type is Switch-Id, long value is -738197487
*Nov 15 12:37:24.559: SSS INFO: Element type is Nasport, ptr value is 63C0E590
*Nov 15 12:37:24.559: SSS INFO: Element type is AAA-Id, long value is 19
*Nov 15 12:37:24.559: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:24.559: SSS PM [uid:18]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:37:24.559: SSS PM [uid:18]: Received Service Request
*Nov 15 12:37:24.559: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy requires 'Unauth-User' key
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy reply - Need more keys
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Got reply Need-More-Keys from PM
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling More-Keys event
*Nov 15 12:37:24.559: [18]PPPoE 15: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:37:24.559: [18]PPPoE 15: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.559: ppp18 PPP: Using default call direction
*Nov 15 12:37:24.559: ppp18 PPP: Treating connection as a dedicated line
*Nov 15 12:37:24.559: ppp18 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:37:24.559: ppp18 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:37:24.559: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.559: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:24.559: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:24.559: [18]PPPoE 15: State START_PPP    Event DYN_BIND
*Nov 15 12:37:24.559: [18]PPPoE 15: data path set to PPP
*Nov 15 12:37:24.563: ppp18 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:24.563: ppp18 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:37:26.523: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.523: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:37:26.527: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.527: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.575: ppp18 LCP: TIMEout: State ACKsent
*Nov 15 12:37:26.575: ppp18 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP:    MRU 1492 (0x010405D4)
```

```
*Nov 15 12:37:26.575: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.575: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: State is Open
*Nov 15 12:37:26.575: ppp18 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:37:26.575: ppp18 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:37:26.579: ppp18 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
Nov 15 12:37:26.579: ppp18 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:37:26.579: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Nov 15 12:37:26.579: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
*Nov 15 12:37:26.579: SSS INFO: Element type is AAA-Id, long value is 19
Nov 15 12:37:26.579: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:37:26.579: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:26.579: SSS PM [uid:18]: Received More Keys
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling AAA service Authorization
*Nov 15 12:37:26.579: SSS PM [uid:18]: Sending authorization request for 'example.com'
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Authorizing key example.com
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:AAA request sent for key example.com
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Received an AAA failure
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <service not found>, state
changed from authorizing to complete
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:No service authorization info found
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Free request
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Next Authorization Check
*Nov 15 12:37:26.587: SSS PM [uid:18]: Default policy: SGF author not needed
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Default Service
*Nov 15 12:37:26.587: SSS PM [uid:18]: Policy reply - Local terminate
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Got reply Local-Term from PM
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Handling Send-Client-Local-Term event
*Nov 15 12:37:26.591: ppp18 PPP: Phase is AUTHENTICATING, Unauthenticated User
Nov 15 12:37:26.595: ppp18 CHAP: O FAILURE id 1 len 25 msg is "Authentication
failed"
*Nov 15 12:37:26.599: ppp18 PPP: Sending Acct Event[Down] id[13]
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: ppp18 LCP: O TERMREQ [Open] id 3 len 4
*Nov 15 12:37:26.599: ppp18 LCP: State is Closed
*Nov 15 12:37:26.599: ppp18 PPP: Phase is DOWN
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: [18]PPPoE 15: State LCP_NEGO    Event PPP_DISCNCT
*Nov 15 12:37:26.599: [18]PPPoE 15: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: AAA account stopped
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Processing a client disconnect
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Handling Send-Service-Disconnect event
```

Troubleshooting the Subscriber Service Switch on the LAC--Authentication Failure Example

The following is sample output indicating call failure due to authentication failure at the LNS:

```
*Nov 15 12:45:02.067: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
```

```
*Nov 15 12:45:02.071: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE : encap string prepared
*Nov 15 12:45:02.071: [21]PPPoE 18: Access IE handle allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: pppoe SSS switch updated
*Nov 15 12:45:02.071: PPPoE 18: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA unique ID allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: No AAA accounting method list
*Nov 15 12:45:02.071: [21]PPPoE 18: Service request sent to SSS
*Nov 15 12:45:02.071: [21]PPPoE 18: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:45:02.091: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:45:02.091: SSS INFO: Element type is Switch-Id, long value is 1946157076
*Nov 15 12:45:02.091: SSS INFO: Element type is Nasport, ptr value is 63B34170
*Nov 15 12:45:02.091: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:02.091: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:02.091: SSS PM [uid:21]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:45:02.091: SSS PM [uid:21]: Received Service Request
*Nov 15 12:45:02.091: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy requires 'Unauth-User' key
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy reply - Need more keys
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Got reply Need-More-Keys from PM
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling More-Keys event
*Nov 15 12:45:02.091: [21]PPPoE 18: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:45:02.091: [21]PPPoE 18: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.091: ppp21 PPP: Using default call direction
*Nov 15 12:45:02.091: ppp21 PPP: Treating connection as a dedicated line
*Nov 15 12:45:02.091: ppp21 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:45:02.091: ppp21 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:45:02.091: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:02.091: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:02.091: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:02.091: [21]PPPoE 18: State START_PPP    Event DYN_BIND
*Nov 15 12:45:02.091: [21]PPPoE 18: data path set to PPP
*Nov 15 12:45:02.095: ppp21 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:    MRU 1492 (0x010405D4
*Nov 15 12:45:02.095: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.095: ppp21 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:02.095: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.315:   Tnl41436 L2TP: I StopCCN from rp1 tnl 31166
*Nov 15 12:45:02.315:   Tnl41436 L2TP: Shutdown tunnel
*Nov 15 12:45:02.315:   Tnl41436 L2TP: Tunnel state change from no-sessions-left to
idle
*Nov 15 12:45:04.055: ppp21 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:45:04.055: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.059: ppp21 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:45:04.059: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.079: ppp21 LCP: TIMEout: State ACKsent
*Nov 15 12:45:04.079: ppp21 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:45:04.079: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:04.079: ppp21 LCP: I CONFACK [ACKsent] id 2 len 19
```

```
*Nov 15 12:45:04.079: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:04.079: ppp21 LCP: State is Open
*Nov 15 12:45:04.079: ppp21 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:45:04.079: ppp21 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:45:04.083: ppp21 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
*Nov 15 12:45:04.083: ppp21 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:45:04.083: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Nov 15 12:45:04.083: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:04.083: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:04.083: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:45:04.083: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:04.083: SSS PM [uid:21]: Received More Keys
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling AAA service Authorization
*Nov 15 12:45:04.083: SSS PM [uid:21]: Sending authorization request for 'example.com'
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Authorizing key example.com
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:AAA request sent for key example.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Received an AAA pass
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Found service info for key example.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Free request
*Nov 15 12:45:04.095: SSS PM [uid:21]: Handling Service Direction
*Nov 15 12:45:04.095: SSS PM [uid:21]: Policy reply - Forwarding
*Nov 15 12:45:04.095: SSS MGR [uid:21]: Got reply Forwarding from PM
*Nov 15 12:45:04.099: SSS MGR [uid:21]: Handling Connect-Service event
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Event connect req, state changed from idle
to connecting
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Requesting connection
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Call request sent
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Event client connect, state changed from
idle to connecting
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Initiating compulsory connection to
192.168.8.2
*Nov 15 12:45:04.099:   Tnl/Sn31399/10 L2TP: Session FS enabled
*Nov 15 12:45:04.099:   Tnl/Sn31399/10 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:45:04.099: uid:21  Tnl/Sn31399/10 L2TP: Create session
*Nov 15 12:45:04.099:   Tnl31399 L2TP: SM State idle
*Nov 15 12:45:04.099:   Tnl31399 L2TP: O SCCRQ
*Nov 15 12:45:04.099:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.099:   Tnl31399 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Nov 15 12:45:04.099:   Tnl31399 L2TP: SM State wait-ctl-reply
*Nov 15 12:45:04.099: [21]PPPoE 18: State LCP_NEGO    Event PPP_FWDING
*Nov 15 12:45:04.107:   Tnl31399 L2TP: I SCCRP from rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Got a challenge from remote peer, rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Got a response from remote peer, rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Tunnel Authentication success
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Tunnel state change from wait-ctl-reply to
established
*Nov 15 12:45:04.107:   Tnl31399 L2TP: O SCCCN  to rp1 tnlid 9349
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.107:   Tnl31399 L2TP: SM State established
```

```
*Nov 15 12:45:04.107: uid:21  Tnl/Sn31399/10 L2TP: O ICRQ to rp1 9349/0
*Nov 15 12:45:04.107: [21]PPPoE 18: Access IE nas port called
*Nov 15 12:45:04.107: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
wait-for-tunnel to wait-reply
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: O ICCN to rp1 9349/13589
*Nov 15 12:45:04.115:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
wait-reply to established
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: VPDN session up
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Event peer connected, state changed from
connecting to connected
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Succeed to forward nobody@example.com
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: accounting start sent
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Connection succeeded
*Nov 15 12:45:04.115: SSS MGR [uid:21]: Handling Service-Connected event
*Nov 15 12:45:04.115: ppp21 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:45:04.115: [21]PPPoE 18: State LCP_NEGO    Event PPP_FWDED
*Nov 15 12:45:04.115: [21]PPPoE 18: data path set to SSS Switch
*Nov 15 12:45:04.119: [21]PPPoE 18: Connected Forwarded
*Nov 15 12:45:04.119: ppp21 PPP: Process pending packets
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Result code(2): 2: Call
disconnected, refer to error msg
*Nov 15 12:45:04.139:      Error code(6): Vendor specific
*Nov 15 12:45:04.139:      Optional msg: Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: I CDN from rp1 tnl 9349, cl
13589
01:06:21: %VPDN-6-CLOSED: L2TP LNS 192.168.8.2 closed  user nobody@example.com; Result
2, Error 6, Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: disconnect (L2X) IETF:
18/host-request Ascend: 66/VPDN Local PPP Disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Destroying session
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
established to idle
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Event peer disconnect, state changed from
connected to disconnected
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Remote disconnected nobody@example.com
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: accounting stop sent
*Nov 15 12:45:04.139:   Tnl31399 L2TP: Tunnel state change from established to
no-sessions-left
*Nov 15 12:45:04.143:   Tnl31399 L2TP: No more sessions in tunnel, shutdown (likely)
in 15 seconds
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event server disc, state changed from
connected to disconnected
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Server disconnected call
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event free req, state changed from
disconnected to terminal
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Free request
*Nov 15 12:45:04.143: SSS MGR [uid:21]: Handling Send Client Disconnect
*Nov 15 12:45:04.143: [21]PPPoE 18: State CNCT_FWDED    Event SSS_DISCNCT
*Nov 15 12:45:04.143: ppp21 PPP: Sending Acct Event[Down] id[16]
*Nov 15 12:45:04.143: ppp21 PPP: Phase is TERMINATING
*Nov 15 12:45:04.143: ppp21 LCP: State is Closed
*Nov 15 12:45:04.143: ppp21 PPP: Phase is DOWN
*Nov 15 12:45:04.143: [21]PPPoE 18: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
```

```
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA account stopped
*Nov 15 12:45:14.139:   Tnl31399 L2TP: I StopCCN from rp1 tnl 9349
*Nov 15 12:45:14.139:   Tnl31399 L2TP: Shutdown tunnel
*Nov 15 12:45:14.139:   Tnl31399 L2TP: Tunnel state change from no-sessions-left
```

Troubleshooting the Subscriber Service Switch on the LNS--Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LNS:

```
Router# debug sss event
Router# debug sss error
Router# debug sss fsm
Router# debug ppp negotiation
Router# debug vpdn l2x-events
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn sss fsm
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
PPP:
  PPP protocol negotiation debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
  VPDN SSS FSM debugging is on
3d17h:   Tnl9264 L2TP: I ICRQ from server1 tnl 61510
3d17h:   Tnl/Sn9264/13586 L2TP: Session FS enabled
3d17h:   Tnl/Sn9264/13586 L2TP: Session state change from idle to wait-connect
3d17h:   Tnl/Sn9264/13586 L2TP: New session created
3d17h:   Tnl/Sn9264/13586 L2TP: O ICRP to server1 61510/7
3d17h:   Tnl9264 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl/Sn9264/13586 L2TP: I ICCN from server1 tnl 61510, cl 7
3d17h: nobody@example.com  Tnl/Sn9264/13586 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:707]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is 1493172561
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1
3d17h: SSS INFO: Element type is AAA-Id, long value is 16726
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is D1000167
3d17h: SSS MGR [uid:707]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:707]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:707]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: SGF author not needed
3d17h: SSS PM [uid:707]: No more authorization methods left to try, providing
default service
3d17h: SSS PM [uid:707]: Received Service Request
3d17h: SSS PM [uid:707]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:707]: Handling Service Direction
3d17h: SSS PM [uid:707]: Policy reply - Local terminate
3d17h: SSS MGR [uid:707]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:707]: Event policy-connect local, state changed from
```

```
wait-for-auth to connected
3d17h: SSS MGR [uid:707]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from SSS to PPP
3d17h: ppp707 PPP: Phase is ESTABLISHING
3d17h: ppp707 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp707 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp707 LCP:    AuthProto CHAP (0x0305C22305)
3d17h: ppp707 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
3d17h: ppp707 LCP: I FORCED sent CONFACK len 10
3d17h: ppp707 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp707 LCP:    MagicNumber 0x0017455D (0x05060017455D)
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp707 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event vaccess resp, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event stat bind resp, state changed from PPP to CNCT
3d17h: Vi4.2  Tnl/Sn9264/13586 L2TP: Session state change from
wait-for-service-selection to established
3d17h: Vi4.2 PPP: Phase is AUTHENTICATING, Authenticated User
3d17h: Vi4.2 CHAP: O SUCCESS id 1 len 4
3d17h: Vi4.2 PPP: Phase is UP
3d17h: Vi4.2 IPCP: O CONFREQ [Closed] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 172.16.0.0 (0x030681010000)
3d17h: Vi4.2 PPP: Process pending packets
3d17h: Vi4.2 IPCP: I CONFREQ [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 10.0.0.0 (0x030600000000)
3d17h: Vi4.2 AAA/AUTHOR/IPCP: Start.  Her address 10.0.0.0, we want 10.0.0.0
3d17h: Vi4.2 AAA/AUTHOR/IPCP: Done.  Her address 10.0.0.0, we want 10.0.0.0
3d17h: Vi4.2 IPCP: Pool returned 10.1.1.3
3d17h: Vi4.2 IPCP: O CONFNAK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: I CONFACK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 172.16.0.0 (0x030681010000)
3d17h: Vi4.2 IPCP: I CONFREQ [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: O CONFACK [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: State is Open
3d17h: Vi4.2 IPCP: Install route to 10.1.1.3
```

Troubleshooting the Subscriber Service Switch on the LNS--Tunnel Failure Example

The following is sample output indicating tunnel failure on the LNS:

```
3d17h: L2TP: I SCCRQ from server1 tnl 31399
3d17h:   Tnl9349 L2TP: Got a challenge in SCCRQ, server1
3d17h:   Tnl9349 L2TP: New tunnel created for remote server1, address 192.168.8.1
3d17h:   Tnl9349 L2TP: O SCCRP  to server1 tnlid 31399
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl9349 L2TP: Tunnel state change from idle to wait-ctl-reply
3d17h:   Tnl9349 L2TP: I SCCCN from server1 tnl 31399
3d17h:   Tnl9349 L2TP: Got a Challenge Response in SCCCN from server1
3d17h:   Tnl9349 L2TP: Tunnel Authentication success
3d17h:   Tnl9349 L2TP: Tunnel state change from wait-ctl-reply to established
3d17h:   Tnl9349 L2TP: SM State established
3d17h:   Tnl9349 L2TP: I ICRQ from server1 tnl 31399
3d17h:   Tnl/Sn9349/13589 L2TP: Session FS enabled
3d17h:   Tnl/Sn9349/13589 L2TP: Session state change from idle to wait-connect
3d17h:   Tnl/Sn9349/13589 L2TP: New session created
3d17h:   Tnl/Sn9349/13589 L2TP: O ICRP to server1 31399/10
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
```

```
3d17h:   Tnl/Sn9349/13589 L2TP: I ICCN from server1 tnl 31399, cl 10
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:709]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is -1912602284
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1
3d17h: SSS INFO: Element type is AAA-Id, long value is 16729
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is 8D00016A
3d17h: SSS MGR [uid:709]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:709]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:709]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: SGF author not needed
d17h: SSS PM [uid:709]: No more authorization methods left to try, providing default
service
3d17h: SSS PM [uid:709]: Received Service Request
3d17h: SSS PM [uid:709]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:709]: Handling Service Direction
3d17h: SSS PM [uid:709]: Policy reply - Local terminate
3d17h: SSS MGR [uid:709]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:709]: Event policy-connect local, state changed from
wait-for-auth to connected
3d17h: SSS MGR [uid:709]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:709]: Event connect local, state changed from SSS to PPP
3d17h: ppp709 PPP: Phase is ESTABLISHING
3d17h: ppp709 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp709 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp709 LCP:    AuthProto CHAP (0x0305C22305)
3d17h: ppp709 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
3d17h: ppp709 LCP: I FORCED sent CONFACK len 10
3d17h: ppp709 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp709 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
3d17h: ppp709 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:709]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp709 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp709 CHAP: O FAILURE id 1 len 25 msg is "Authentication failed"
3d17h: ppp709 PPP: Sending Acct Event[Down] id[4159]
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: ppp709 LCP: O TERMREQ [Open] id 1 len 4
3d17h: ppp709 LCP: State is Closed
3d17h: ppp709 PPP: Phase is DOWN
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: VPDN SSS [uid:709]: Event peer disc, state changed from PPP to DSC
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: disconnect (AAA) IETF:
17/user-error Ascend: 26/PPP CHAP Fail
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: O CDN to server1 31399/10
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Destroying session
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Session state change from
wait-for-service-selection to idle
3d17h: VPDN SSS [uid:709]: Event vpdn disc, state changed from DSC to END
3d17h:   Tnl9349 L2TP: Tunnel state change from established to no-sessions-left
3d17h:   Tnl9349 L2TP: No more sessions in tunnel, shutdown (likely) in 10 seconds
3d17h: SSS MGR [uid:709]: Processing a client disconnect
3d17h: SSS MGR [uid:709]: Event client-disconnect, state changed from connected to
end
3d17h: SSS MGR [uid:709]: Handling Send-Service-Disconnect event
3d17h:   Tnl9349 L2TP: O StopCCN  to server1 tnlid 31399
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
```

```
3d17h:   Tnl9349 L2TP: Tunnel state change from no-sessions-left to shutting-down
3d17h:   Tnl9349 L2TP: Shutdown tunnel
```

Where to Go Next

- If you want to establish PPPoE session limits for sessions on a specific permanent virtual circuit or VLAN configured on an L2TP access concentrator, refer to the "Establishing PPPoE Session Limits per NAS Port" module.
- If you want to use service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup, refer to the "Offering PPPoE Clients a Selection of Services During Call Setup" module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over a L2TP control channel to an LNS or tunnel switch, refer to the "Enabling PPPoE Relay Discovery and Service Selection Functionality" module.
- If you want to configure a transfer upstream of the PPPoX session speed value, refer to the "Configuring Upstream Connections Speed Transfer" module.
- If you want to use the Simple Network Management Protocol (SNMP) to monitor PPPoE sessions, refer to the "Monitoring PPPoE Sessions with SNMP" module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, refer to the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, see the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

The following sections provide references related to configuring Cisco Subscriber Service Switch policies.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation module
Tasks for preparing for broadband access aggregation.	Preparing for Broadband Access Aggregation module
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Configuration procedure for PPPoE.	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions
Configuration procedures for PPPoA.	Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2661	Layer Two Tunneling Protocol L2TP
RFC 2341	Cisco Layer Two Forwarding (Protocol) L2F
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE) (PPPoE Discovery)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

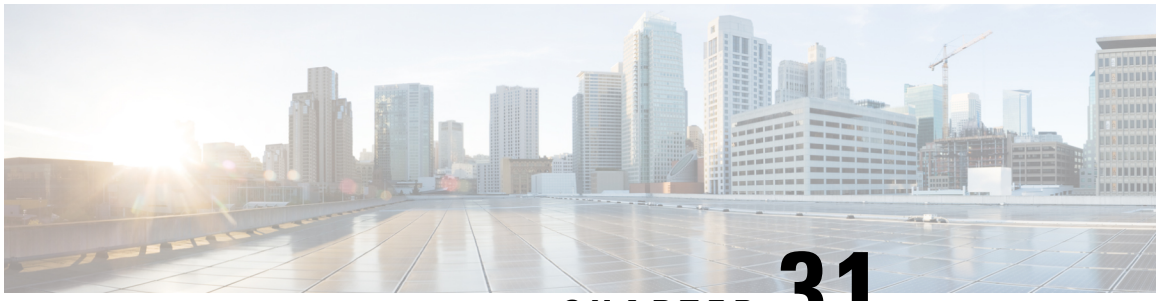
Feature Information for Configuring a Subscriber Service Switch Policy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 37: Feature Information for Configuring a Cisco Subscriber Service Switch Policy

Feature Name	Releases	Feature Configuration Information
Subscriber Service Switch	Cisco IOS XE Release 2.1	The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. The primary purpose of the Subscriber Service Switch is to direct PPP from one point to another using a Layer 2 subscriber policy. This feature was integrated into Cisco IOS XE Release 2.1.



CHAPTER 31

AAA Improvements for Broadband IPv6

This feature provides AAA improvements for Broadband IPv6 support.

Information About AAA Improvements for Broadband IPv6

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are inacl, outacl, prefix, and route.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

AAA Support for IPv6 RADIUS Attributes

The following RADIUS attributes, as described in RFC 3162, are supported for IPv6:

- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Login-IPv6-Host

The following RADIUS attributes are also supported for IPv6:

- Delegated-IPv6-Prefix (RFC 4818)
- Delegated-IPv6-Prefix-Pool

- DNS-Server-IPv6-Address
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route

The attributes listed above can be configured on a RADIUS server and downloaded to access servers, where they can be applied to access connections.

Prerequisites for Using AAA Attributes for IPv6

AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162.

RADIUS Per-User Attributes for Virtual Access in IPv6 Environments

The following IPv6 RADIUS attributes are supported for virtual access and can be used as attribute-value (AV) pairs:

- Delegated-IPv6-Prefix
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route
- Login-IPv6-Host

Delegated-IPv6-Prefix

The Delegated-IPv6-Prefix attribute indicates an IPv6 prefix to be delegated to a user for use in a network. This attribute is used during DHCP prefix delegation between a RADIUS server and a delegating device. A Network Access Server (NAS) that hosts a DHCP Version 6 (DHCPv6) server can act as a delegating device.

The following example shows how to use the Delegated-IPv6-Prefix attribute:

```
ipv6:delegated-prefix=2001:DB8::/64
```

Note The Cisco VSA format is not supported for this attribute. If you try to add this attribute in the Cisco VSA format into a user profile, the RADIUS server response fails. Use only the IETF attribute format for this attribute.

Delegated-IPv6-Prefix-Pool

The Delegated-IPv6-Prefix-Pool attribute indicates the name of a prefix pool from which a prefix is selected and delegated to a device.

Prefix delegation is a DHCPv6 option for delegating IPv6 prefixes. Prefix delegation involves a delegating device that selects a prefix and assigns it on a temporary basis to a requesting device. A delegating device uses many strategies to choose a prefix. One method is to choose a prefix from a prefix pool with a name that is defined locally on a device.

The Delegated-IPv6-Prefix-Pool attribute indicates the name of an assigned prefix pool. A RADIUS server uses this attribute to communicate the name of a prefix pool to a NAS hosting a DHCPv6 server and acting as a delegating device.

You may use DHCPv6 prefix delegation along with ICMPv6 stateless address autoconfiguration (SLAAC) on a network. In this case, both the Delegated-IPv6-Prefix-Pool attribute and the Framed-IPv6-Pool attribute may be included within the same packet. To avoid ambiguity, the Delegated-IPv6-Prefix-Pool attribute should be restricted to the authorization and accounting of prefix pools used in DHCPv6 delegation, and the Framed-IPv6-Pool attribute should be used for the authorization and accounting of prefix pools used in SLAAC.

The following example shows how an address prefix is selected from a pool named pool1. The prefix pool pool1 is downloaded to a delegating device from a RADIUS server by using the Delegated-IPv6-Prefix-Pool attribute. The device then selects the address prefix 2001:DB8::/64 from this prefix pool.

```
Cisco:Cisco-AVpair = "ipv6:delegated-ipv6-pool = pool1"
!
ipv6 dhcp pool pool1
address prefix 2001:DB8::/64
!
```

DNS-Server-IPv6-Address

The DNS-Server-IPv6-Address attribute indicates the IPv6 address of a Domain Name System (DNS) server. A DHCPv6 server can configure a host with the IPv6 address of a DNS server. The IPv6 address of the DNS server can also be conveyed to the host using router advertisement messages from ICMPv6 devices.

A NAS may host a DHCPv6 server to handle DHCPv6 requests from hosts. The NAS may also act as a device that provides router advertisement messages. Therefore, this attribute is used to provide the NAS with the IPv6 address of the DNS server.

If a NAS has to announce more than one recursive DNS server to a host, this attribute can be included multiple times in Access-Accept packets sent from the NAS to the host.

The following example shows how you can define the IPv6 address of a DNS server by using the DNS-Server-IPv6-Address attribute:

```
Cisco:Cisco-AVpair = "ipv6:ipv6-dns-servers-addr=2001:DB8::"
```

Framed-Interface-Id

The Framed-Interface-Id attribute indicates an IPv6 interface identifier to be configured for a user.

This attribute is used during IPv6 Control Protocol (IPv6CP) negotiations of the Interface-Identifier option. If negotiations are successful, the NAS uses this attribute to communicate a preferred IPv6 interface identifier to the RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets.

Framed-IPv6-Pool

The Framed-IPv6-Pool attribute indicates the name of a pool that is used to assign an IPv6 prefix to a user. This pool should be either defined locally on a device or defined on a RADIUS server from where pools can be downloaded.

Framed-IPv6-Prefix

The Framed-IPv6-Prefix attribute indicates an IPv6 prefix (and a corresponding route) to be configured for a user. So this attribute performs the same function as a Cisco VSA and is used for virtual access only. A NAS uses this attribute to communicate a preferred IPv6 prefix to a RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets and can appear multiple times in these packets. The NAS creates a corresponding route for the prefix.

This attribute is used by a user to specify which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol.

This attribute can also be used for DHCPv6 prefix delegation, and a separate profile must be created for a user on the RADIUS server. The username associated with this separate profile has the suffix “-dhcpv6”.

The Framed-IPv6-Prefix attribute is treated differently in this separate profile and the regular profile of a user. If a NAS needs to send a prefix through router advertisement messages, the prefix is placed in the Framed-IPv6-Prefix attribute of the regular profile of the user. If a NAS needs to delegate a prefix to the network of a remote user, the prefix is placed in the Framed-IPv6-Prefix attribute of the separate profile of the user.

Note The RADIUS IETF attribute format and the Cisco VSA format are supported for this attribute.

Framed-IPv6-Route

The Framed-IPv6-Route attribute indicates the routing information to be configured for a user on a NAS. This attribute performs the same function as a Cisco VSA. The value of the attribute is a string and is specified by using the **ipv6 route** command.

IPv6 ACL

The IPv6 ACL attribute is used to specify a complete IPv6 access list. The unique name of an access list is generated automatically. An access list is removed when the respective user logs out. The previous access list on the interface is then reapplied.

The inacl and outacl attributes enable you to specify an existing access list configured on a device. The following example shows how to define an access list identified with number 1:

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6_DNS_Servers

The IPv6_DNS_Servers attribute is used to send up to two DNS server addresses to the DHCPv6 server. The DNS server addresses are saved in the interface DHCPv6 subblock and override other configurations in the DHCPv6 pool. This attribute is also included in attributes returned for AAA start and stop notifications.

IPv6 Pool

The IPv6 Pool attribute extends the IPv4 address pool attribute to support the IPv6 protocol for RADIUS authentication. This attribute specifies the name of a local pool on a NAS from which a prefix is chosen and used whenever PPP is configured and the protocol is specified as IPv6. The address pool works with local pooling and specifies the name of a local pool that is preconfigured on the NAS.

IPv6 Prefix#

The IPv6 Prefix# attribute indicates which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol. When this attribute is used, a corresponding route (marked as a per-user static route) is installed in the routing information base (RIB) tables for a given prefix.

The following example shows how to specify which prefixes to advertise:

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

The IPv6 Route attribute is used to specify a static route for a user. A static route is appropriate when Cisco software cannot dynamically build a route to the destination. See the **ipv6 route** command for more information about building static routes.

The following example shows how to use the IPv6 Route attribute to define a static route:

```
cisco-avpair = "ipv6:route#1=2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:route#2=2001:DB8:cc00:2::/48",
```

Login-IPv6-Host

The Login-IPv6-Host attribute indicates IPv6 addresses of hosts with which to connect a user when the Login-Service attribute is included. A NAS uses the Login-IPv6-Host attribute in Access-Request packets to communicate to a RADIUS server that it prefers to use certain hosts.

How to Enable AAA Improvements for Broadband IPv6

Sending IPv6 Counters to the Accounting Server

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **aaa accounting send counters ipv6**

DETAILED STEPS

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 **aaa accounting send counters ipv6**

Example:

```
Device(config)# aaa accounting send counters ipv6
```

Sends IPv6 counters in the stop record to the accounting server.

Configuration Examples for AAA Improvements for Broadband IPv6

Example: Sending IPv6 Counters to the Accounting Server

```
Device# show running-config
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting send counters ipv6
aaa accounting network default
 action-type start-stop
 group radius
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco_IOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

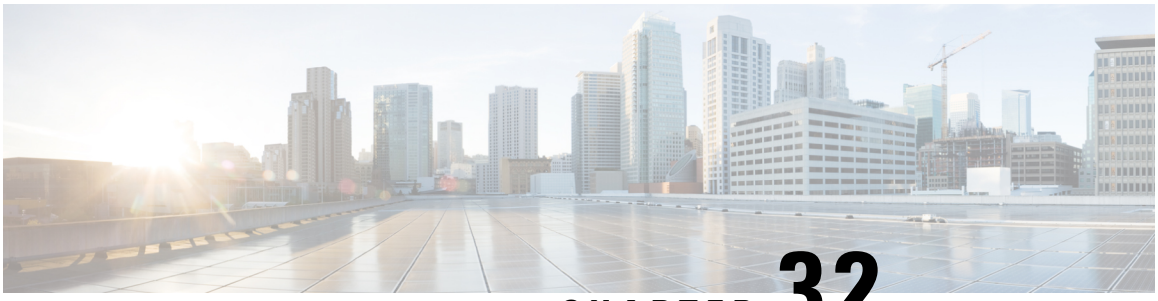
Feature Information for AAA Improvements for Broadband IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 38: Feature Information for AAA Improvements for Broadband IPv6

Feature Name	Releases	Feature Information
AAA Improvements for Broadband IPv6	Cisco IOS XE Release 2.5	The AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162. The following commands were introduced or modified: **aaa accounting send counters ipv6**.



CHAPTER 32

Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

The Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS feature enables you to shape PPP over Ethernet over VLAN sessions to a user-specified rate. The router shapes the sum of all of the traffic to the PPPoE session so that the subscriber's connection to the digital subscriber line access multiplexer (DSLAM) does not become congested. Queueing-related functionality provides different levels of service to the various applications that execute over the PPPoE session.

A nested, two-level hierarchical service policy is used to configure session shaping directly on the router using the modular quality of service command-line interface (MQC). The RADIUS server applies the service policy to a particular PPPoE session by downloading a RADIUS attribute to the router. This attribute specifies the policy map name to apply to the session. RADIUS notifies the router to apply the specified policy to the session. Because the service policy contains queueing-related actions, the router sets up the appropriate class queues and creates a separate versatile traffic management and shaping (VTMS) system link dedicated to the PPPoE session.

Restrictions for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

- Each PPPoE over VLAN session for which per session queueing and shaping is configured has its own set of queues and its own VTMS link. Therefore, these PPPoE sessions do not inherit policies unless you remove the service policy applied to the session or you do not configure a policy for the session.
- The router supports per session queueing and shaping on PPPoE terminated sessions and on an IEEE 802.1Q VLAN tagged subinterfaces for outbound traffic only.

- The router does not support per session queueing and shaping for PPPoE over VLAN sessions using RADIUS on inbound interfaces.
- The router does not support per session queueing and shaping for layer 2 access concentrator (LAC) sessions.
- The statistics related to quality of service (QoS) that are available using the **show policy-map interface** command are not available using RADIUS.
- The router does not support using a virtual template interface to apply a service policy to a session.
- You can apply per session queueing and shaping policies only as output service policies. The router supports input service policies on sessions for other existing features, but not for per session queueing and shaping for PPPoE over VLAN using RADIUS.
- During periods of congestion, the router does not provide specific scheduling between the various PPPoE sessions. If the entire port becomes congested, the scheduling that results has the following effects:
  - The amount of bandwidth that each session receives of the entire port's capacity is not typically proportionally fair share.
  - The contribution of each class queue to the session's total bandwidth might not degrade proportionally.
- The PRE2 does not support ATM overhead accounting for egress packets with Ethernet encapsulations. Therefore, the router does not consider ATM overhead calculations when determining that the shaping rate conforms to contracted subscriber rates.
- The router does not support the configuration of the policy map using RADIUS. You must use the MQC to configure the policy map on the router.

Information About Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

The router allows you to apply QoS policy maps using RADIUS. The actual configuration of the policy map occurs on the router using the MQC.

How Routers Apply QoS Policy to Sessions

The router can apply the QoS policy to sessions using attributes defined in one of the following RADIUS profiles:

- User Profile--The user profile on the RADIUS server contains an entry that identifies the policy map name applicable to the user. The policy map name is the service that RADIUS downloads to the router after a session is authorized.
- Service Profile--The service profile on the RADIUS server specifies a session identifier and an attribute-value (AV) pair. The session identifier might be, for example, the IP address of the session. The AV-pair defines the service (policy map name) to which the user belongs.

The following AV-pairs define the QoS policy to be applied dynamically to the session:

"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"

"ip:sub-qos-policy-out=<name of egress policy>"

When RADIUS gets a service-logon request from the policy server, it sends a change of authorization (CoA) request to the router to activate the service for the subscriber, who is already logged in.

If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the above attribute and applies the QoS policy to the session.

Note Although the router also supports the RADIUS VSA 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the above attributes for QoS policy definitions.

How RADIUS Uses VSA 38 in User Profiles

The RADIUS VSA 38 is used for downstream traffic going toward a subscriber. The service (policy map name) to which the user session belongs resides on the RADIUS server. The router downloads the name of the policy map from RADIUS using VSA 38 in the user profile and then applies the policy to the session.

To set up RADIUS for per session queueing and shaping for PPPoE over VLAN support, enter the following VSA in the user profile on the RADIUS server:

```
Cisco:Cisco-Policy-Down = <service policy name>
```

The actual configuration of the policy map occurs on the router. The user profile on the RADIUS service contains an entry that identifies the policy map name applicable to the user. This policy map name is the service RADIUS downloads to the router using VSA 38.

Note Although the router also supports RADIUS VSA 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the attributes described in the How Routers Apply QoS Policy to Sessions, on page 370 for QoS policy definitions.

Commands Used to Define QoS Actions

When you configure queueing and shaping for PPPoE over VLAN sessions, the child policy of a nested hierarchical service policy defines QoS actions using any of the following QoS commands:

- **priority** command--Assigns priority to a traffic class and gives preferential treatment to the class.
- **bandwidth** command--Enables class-based fair queueing and creates multiple class queues based on bandwidth.
- **queue-limit** command--Specifies the maximum number of packets that a particular class queue can hold.
- **police** command--Regulates traffic based on bits per second (bps), using the committed information rate (CIR) and the peak information rate, or on the basis of a percentage of bandwidth available on an interface.
- **random-detect** command--Drops packets based on a specified value to control congestion before a queue reaches its queue limit. The drop policy is based on IP precedence, differentiated services code point (DSCP), or the discard-class.

- **set ip precedence** command--Marks a packet with the IP precedence level you specify.
- **set dscp** command--Marks a packet with the DSCP you specify.
- **set cos** command--Sets the IEEE 802.1Q class of service bits in the user priority field.

The parent policy contains only the class-default class with the **shape** command configured. This command shapes traffic to the specified bit rate, according to a specific algorithm.

The router allows you to apply QoS policy maps using RADIUS. The actual configuration of the policy map occurs on the router using the MQC. The router can apply the QoS policy to sessions using attributes defined in one of the following RADIUS profiles:

- User Profile--The user profile on the RADIUS server contains an entry that identifies the policy map name applicable to the user. The policy map name is the service that RADIUS downloads to the router after a session is authorized.
- Service Profile--The service profile on the RADIUS server specifies a session identifier and an attribute-value (AV) pair. The session identifier might be, for example, the IP address of the session. The AV-pair defines the service (policy map name) to which the user belongs.

The following AV-pairs define the QoS policy to be applied dynamically to the session:

"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"

"ip:sub-qos-policy-out=<name of egress policy>"

When RADIUS gets a service-logon request from the policy server, it sends a change of authorization (CoA) request to the router to activate the service for the subscriber, who is already logged in.

If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the above attribute and applies the QoS policy to the session.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the above attributes for QoS policy definitions.

How to Use the Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS Feature

Configuring a Per Session Queueing and Shaping Policy on the Router

To configure a per session queueing and shaping policy on the router for PPPoE over VLAN sessions using RADIUS, you must complete the following steps.

SUMMARY STEPS

1. **policy-map** *policy-map-name*
2. **class**

3. **bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} **account**{{**qinq**| **dot1q**} {**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}}
4. exit
5. **policy-map** *policy-map-name*
6. **class** *class-default*
7. **shape** *rate* **account** {{{**qinq**| **dot1q**}{**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}}
8. **service-policy** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy-map-name`	Creates or modifies the bottom-level child policy. • *policy-map-name* is the name of the child policy map. The name can be a maximum of 40 alphanumeric characters.
Step 2	**class** **Example:** `Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. • *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions. • Repeat Steps 2 and 3 for each traffic class you want to include in the policy map.
Step 3	**bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} **account**{{**qinq**| **dot1q**} {**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}} **Example:** `Router(config-pmap-c)# bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {aal5 | aal3} subscriber-encapsulation | user-defined offset [atm]}`	Enables class-based fair queueing. • *bandwidth-kbps* specifies or modifies the minimum bandwidth allocated for a class belonging to a policy map. Valid values are from 8 to 2488320, which represents from 1 to 99 percent of the link bandwidth. • **percent** *percentage* specifies or modifies the minimum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **remaining percent** *percentage* specifies or modifies the minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **account** enables ATM overhead accounting. For more information, see the " ATM Overhead Accounting " section of the "Configuring Dynamic Subscriber Services" chapter of the *Cisco 10000 Series Router Quality of Service Configuration Guide*.

	Command or Action	Purpose
		• **qinq** specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **dot1q** specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **aal5** specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. You must specify either **aal5** or aal3. • **aal3** specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**. • *subscriber-encapsulation* specifies the encapsulation type at the subscriber line. • **user-defined** indicates that the router is to use the *offset* you specify when calculating ATM overhead. • *offset* specifies the offset size the router is to use when calculating ATM overhead. Valid values are from -63 to 63 bytes. **Note** The router configures the offset size if you do not specify the *offset* option. • **atm** applies ATM cell tax in the ATM overhead calculation.
Step 4	exit **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 5	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map policy-map-name`	Creates or modifies the parent policy. • *policy-map-name* is the name of the parent policy map. The name can be a maximum of 40 alphanumeric characters.
Step 6	**class** *class-default* **Example:** `Router(config-pmap)# class class-default`	Configures or modifies the parent class-default class. **Note** You can configure only the class-default class in a parent policy. Do not configure any other traffic class.
Step 7	**shape** *rate* **account** {{{**qinq**| **dot1q**}{**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}}	Shapes traffic to the indicated bit rate and enables ATM overhead accounting.

	Command or Action	Purpose
	Example: `Router(config-pmap-c)# shape rate account {qinq | dot1q} {aal5 | aal3} subscriber-encapsulation | {user-defined offset [atm]}`	• *rate* is the bit-rate used to shape the traffic, expressed in kilobits per second. • **account** enables ATM overhead accounting. • **qinq** specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **dot1q** specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **aal5** specifies the ATM Adaptation Layer 5 that supports connection-oriented VBR services. You must specify either **aal5** or **aal3**. • **aal3** specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**. • *subscriber-encapsulation* specifies the encapsulation type at the subscriber line. • **user-defined** indicates that the router is to use the *offset* you specify when calculating ATM overhead. • *offset* specifies the offset size the router is to use when calculating ATM overhead. Valid values are from -63 to 63 bytes. **Note** The router configures the offset size if you do not specify the **user-defined** *offset* option. • **atm** applies ATM cell tax in the ATM overhead calculation.
Step 8	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy policy-map-name`	Applies a bottom-level child policy to the top-level parent class-default class. • *policy-map-name* is the name of the previously configured child policy map.

Verifying Per Session Queueing

To display the configuration of per session queueing and shaping policies for PPPoE over VLAN, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router# show policy-map interface interface`	Displays information about the policy map attached to the interface you specify. If you do not specify an interface, it displays information about all of the policy maps configured on the router. • *interface* specifies the virtual-access interface and number the router created for the session (for example, virtual-access 1).
`Router# show policy-map session uid uid-number`	Displays the session QoS counters for the subscriber session you specify. • **uid** *uid-number* defines a unique session ID. Valid values for *uid-number* are from 1 to 65535.
`Router# show running-config`	Displays the running configuration on the router. The output shows the AAA setup and the configuration of the policy map, ATM VC, PPPoA, dynamic bandwidth selection, virtual template, and RADIUS server.

Configuration Examples for Per Session Queueing and Shaping Policies

Configuring a Per Session Queueing and Shaping Policy on the Router Example

The following example shows

The example creates two traffic classes: Voice and Video. The router classifies traffic that matches IP precedence 5 as Voice traffic and traffic that matches IP precedence 3 as Video traffic. The Child policy map gives priority to Voice traffic and polices traffic at 2400 kbps. The Video class is allocated 80 percent of the remaining bandwidth and has ATM overhead accounting enabled. The Child policy is applied to the class-default class of the Parent policy map, which receives 20 percent of the remaining bandwidth and shapes traffic to 10,000 bps, and has ATM overhead accounting enabled.

```
Router(config)# class-map Voice
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# class-map Video
Router(config-cmap)# match ip precedence 3
!
Router(config)# policy-map Child
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 2400 9216 0 conform-action transmit exceed-action drop
violate-action drop
Router(config-pmap-c)# class video
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-dot1q-rbe
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 10000 account dot1q snap-dot1q-rbe
Router(config-pmap-c)# service-policy Child
```

Setting Up RADIUS for Per Session Queueing and Shaping Example

The following are example configurations for the Merit RADIUS server and the associated Layer 2 network server (LNS). In the example, the Cisco-Policy-Down attribute indicates the name of the policy map to be downloaded, which in this example is rad-output-policy. The RADIUS dictionary file includes an entry for Cisco VSA 38.

```
example.com Password = "cisco123"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Cisco:Cisco-Policy-Down = rad-output-policy
```

Cisco.attr Cisco-Policy-Up 37 string (*, *)

Cisco.attr Cisco-Policy-Down 38 string (*, *)

Verifying Per Session Queueing and Shaping Policies Examples

This example shows sample output for the **show policy-map interface** command

```
Router# show policy-map interface virtual-access 1
!
!
Service-policy output: TEST
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 100/1000
```

This example shows sample output from the **show policy-map session** command and **show policy-map session uid** command, based on a nested hierarchical policy.

```
Router# show subscriber session
Current Subscriber Information: Total sessions 1
Uniq ID Interface  State         Service      Identifier           Up-time
36      Vi2.1      authen        Local Term   peapen@cisco.com     00:01:36
Router# show policy-map parent
  Policy Map parent
    Class class-default
      Average Rate Traffic Shaping
      cir 10000000 (bps)
      service-policy child
Router# show policy-map child

  Policy Map child
    Class voice
      priority
      police 8000 9216 0
       conform-action transmit
       exceed-action drop
       violate-action drop
```

```
    Class video
      bandwidth remaining 80 (%)
Router# show policy-map session uid 36
 SSS session identifier 36 -
 SSS session identifier 36 -
  Service-policy output: parent
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
      Service-policy : child
        queue stats for all priority classes:
          Queueing
          queue limit 16 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: voice (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 5
          Priority: Strict, burst bytes 1500, b/w exceed drops: 0

          Police:
            8000 bps, 9216 limit, 0 extended limit
            conformed 0 packets, 0 bytes; action:
            transmit
            exceeded 0 packets, 0 bytes; action:
            drop
            violated 0 packets, 0 bytes; action:
            drop
        Class-map: video (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 3
          Queueing
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth remaining 80% (7993 kbps)
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 2/136
```

Additional References

The following sections provide references related to the Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS feature.

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

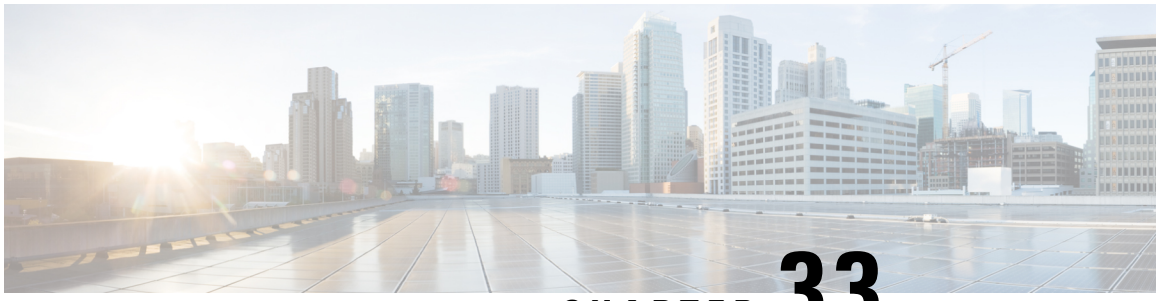
Feature Information for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 39: Feature Information for Per Session Queueing and Shaping for PPPoE over VLAN Using RADIUS

Feature Name	Releases	Feature Information
Per Session Queueing and Shaping for PPPoE over VLAN Using RADIUS	Cisco IOS XE Release 2.1	This feature enables you to shape PPPoE over VLAN sessions to a user-specified rate. The Per Session Queueing and Shaping for PPPoE over VLAN Support Using RADIUS feature was introduced on the PRE2 to enable dynamic queueing and shaping policies on PPPoEoVLAN session. This feature was integrated into Cisco IOS XE Release 2.1.



CHAPTER 33

802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization. This capability enables a way to provide best-effort quality of service (QoS) or class of service (CoS) at Layer 2 without requiring reservation setup.

Prerequisites for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The PPPoE over 802.1Q VLAN feature must be enabled.

Restrictions for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

You cannot set different CoS levels for PPP and Point-to-Point Protocol over Ethernet (PPPoE) control packets; all control packets default to a CoS level set at 0.

Information About 802.1P CoS Bit Set for PPP and PPPoE Control Frames

To configure the 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature, you should understand the following concepts:

The command can help troubleshoot 802.1P control frame marking: **debug pppoe error**

Benefits of 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature facilitates moving from ATM-based to Ethernet-based networks by supporting the ability to offer prioritized traffic services, Voice over Internet Protocol (VoIP), and other premium services.

Feature Design of 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The IEEE 802.1P specification is an extension of the IEEE 802.1Q VLANs tagging standard and enables Layer 2 devices to prioritize traffic by using an 802.1P header that includes a three-bit user priority field. If congestion occurs when the 802.1P CoS bit is not set, PPP keepalive packets can be lost, which can result in disconnection of an established session with loss of service to the end user. Congestion caused by noncontrol packets can also prevent new sessions from being established, which also can result in denying service to the end user.

PPPoE sessions established over 802.1Q VLANs use the priority header field to provide best-effort QoS or CoS at Layer 2 without involving reservation setup. 802.1P traffic is marked and sent to the destination, and no bandwidth reservations are established.

In Cisco IOS XE Release 2.4, PPPoE sessions established over IEEE 802.1Q VLAN make use of the priority field of the IEEE 802.1p header by setting the CoS field to user priority 7.

During network congestion, when the Ethernet network and digital subscriber line access multiplexer (DSLAM) offer 802.1P support, control packets are offered a higher priority than noncontrol packets, thereby increasing the likelihood of reliable delivery. PPPoE control packets and PPP packets originating from the broadband remote access server (BRAS) are marked with user priority 0, the highest level of priority.

The following packets are tagged with user priority 0 in their 802.1P header:

- PPPoE packets
  - PPPoE Active Discovery Offer (PADO)
  - PPPoE Active Discovery Session Confirmation (PADS)
- PPP packets
  - Link Control Protocol (LCP)
  - Network Control Protocol (NCP) (Internet Protocol Control Protocol (IPCP))
  - Authentication
  - Keepalive

How to Configure 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature is enabled by default and requires no configuration.

Configuration Examples for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The following task explains how to change the CoS setting for PPP and PPPoE control frames over 802.1Q VLAN.

Setting 802.1P Priority Bits in 802.1Q Frames Containing PPPoE Control Packets

This task explains how to change the CoS settings for PPP and PPPoE control frames over 802.1Q VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **control-packets vlan cos priority**
5. **exit**
6. **bba-group pppoe group-name**
7. **control-packets vlan cos priority**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe group-name** **Example:**	Specifies the BBA group and enters BBA group configuration mode.

	Command or Action	Purpose
	`Router(config)# bba-group pppoe global`	
Step 4	**control-packets vlan cos priority** **Example:** `Router(config-bba-group)# control-packets vlan cos 5`	Sets the PPPoE control packets associated with the BBA group.
Step 5	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode, and returns to global configuration mode.
Step 6	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe cisco`	Specifies the BBA group cisco and enters BBA group configuration mode.
Step 7	**control-packets vlan cos priority** **Example:** `Router(config-bba-group)# control-packets vlan cos 2`	Sets the PPPoE control packets associated with the BBA group.
Step 8	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode, and returns to global configuration mode.

Additional References

The following sections provide references related to the 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	*Cisco IOS XE Broadband and DSL Configuration Guide*
Broadband access commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
IEEE Standard 802.1P	PPPoE over IEEE 802.1Q
IEEE Standard 802.1Q	Virtual Bridged Local Area Networks

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	PPP over Ethernet

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

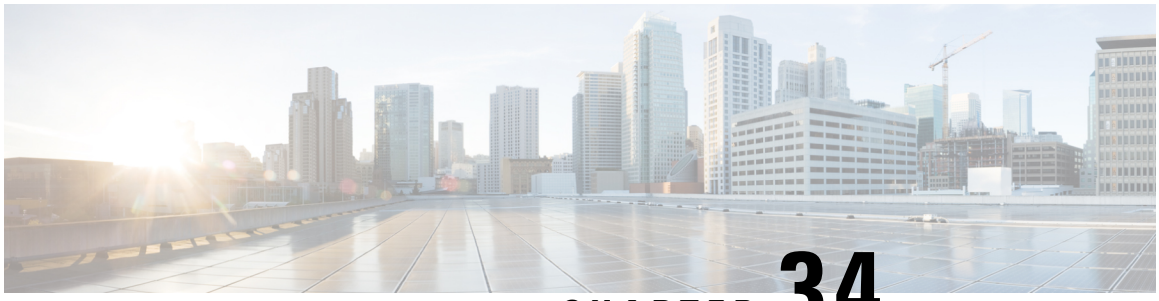
Feature Information for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 40: Feature Information for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

Feature Name	Releases	Feature Information
802.1P CoS Bit Set for PPP and PPPoE Control Frames	Cisco IOS XE Release 2.4	The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization. This capability enables a way to provide best-effort QoS or CoS at Layer 2 without requiring reservation setup. In Cisco IOS XE Release 2.4, this feature was introduced. The following command was introduced: **control-packets vlan cos**.



CHAPTER 34

PPP over Ethernet Client

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers.

PPPoE is a commonly used application in the deployment of digital subscriber lines (DSLs). The PPP over Ethernet Client feature expands PPPoE functionality by providing support for PPPoE on the client and the server.

Prerequisites for PPP over Ethernet Client

PPP connections must be established between two endpoints over a serial link.

Restrictions for PPP over Ethernet Client

The PPPoE client does not support the following:

- More than ten clients per customer premises equipment (CPE)
- Quality of service (QoS) transmission with queueing on the dialer interface
- Dial-on-demand
- Easy VPN
- Native IPv6
- PPPoE client over ATM permanent virtual circuit (PVC)
- You can configure a dial-pool-number on a physical interface or sub-interface using the **pppoe-client dial-pool-number** *pool-number* command.

Note The pool number being unique cannot be used to configure with the same number on any other interfaces.

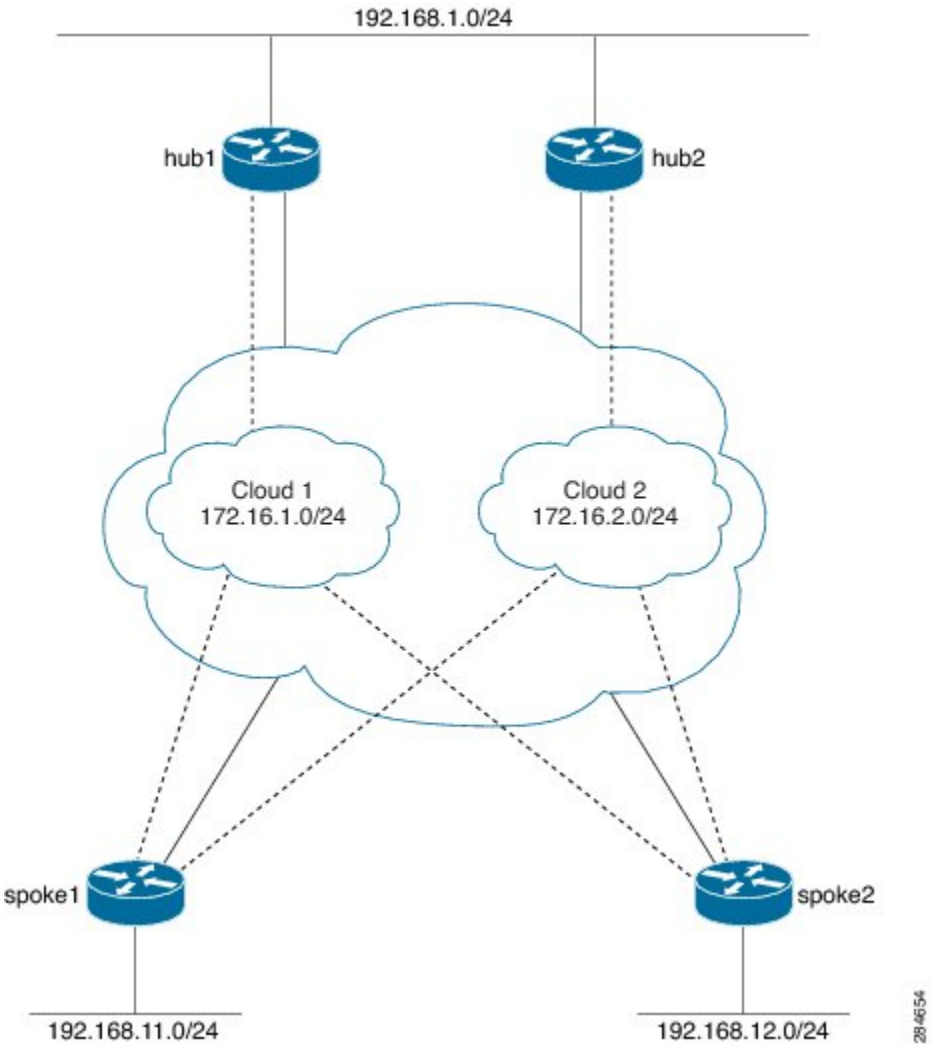
- Co-existence of the PPPoE client and server on the same device.
- Multilink PPP (MLP) on dialer interfaces
- Nonstop forwarding (NSF) with stateful switchover (SSO)
- When an IPv6 address is assigned to a subinterface from a server and if you remove the subinterface on client device, the IPv6 address might not be removed from the interface resulting in a ping failure after reconfiguring the subinterface. This is because you must shut the interface, first and then remove the subinterface.

Information About PPP over Ethernet Client

PPP over Ethernet Client Network Topology

The PPPoE Client feature provides PPPoE client support on routers at customer premises. Before the introduction of this feature, Cisco IOS XE software supported PPPoE only on the access server side. The figure below shows Dynamic Multipoint VPN (DMVPN) access to multiple hosts from the same PPPoE client using a common dialer interface and shared IPsec.

Figure 29: DMVPN Access to Multiple Hosts from the Same PPPoE Client



PPP over Ethernet Client Session Initiation

A PPPoE session is initiated by the PPPoE client. If the session has a timeout or is disconnected, the PPPoE client will immediately attempt to reestablish the session.

The following steps describe the exchange of packets that occurs when a PPPoE client initiates a PPPoE session:

1. The client broadcasts a PPPoE active discovery initiation (PADI) packet.
2. When the access concentrator receives a PADI packet that it can serve, it replies by sending a PPPoE active discovery offer (PADO) packet to the client.
3. Because the PADI packet was broadcast, the host may receive more than one PADO packet. The host looks through the PADO packets it receives and chooses one. The choice can be based on the access concentrator name or on the services offered. The host then sends a single PPPoE active discovery request (PADR) packet to the access concentrator that it has chosen.

4. The access concentrator responds to the PADR packet by sending a PPPoE active discovery session-confirmation (PADS) packet. At this point, a virtual access interface is created that will then negotiate PPP and the PPPoE session will run on this virtual access.

If a client does not receive a PADO packet for a PADI packet already received, the client sends out a PADI packet at predetermined intervals. That interval length is doubled for every successive PADI packet that does not evoke a response, until the interval reaches the configured maximum.

If PPP negotiation fails or the PPP line protocol is brought down for any reason, the PPPoE session and the virtual access will be brought down and the client will wait for a predetermined number of seconds before trying to establish another PPPoE session.

PPPoE Client over VLAN Interface

When configuring a PPPoE client on a VLAN interface, the device sends and receives PADO and PADI packets, but the PPPoE engine does not process PADO packets, and the PPPoE session does not come up. This enhancement provides the option to configure the PPPoE client over a VLAN, such as a Switched Virtual Interface (SVI), and establish the PPPoE session.

Figure 30: Sample Topology of a PPPoE Client and Server over a VLAN Interface

How to Configure PPP over Ethernet Client

Configuring a PPPoE Client

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **pppoe enable group global**
6. **pppoe-client dial-pool-number** *number*
7. **no shutdown**
8. **exit**
9. **interface dialer** *number*
10. **dialer** *pool number*
11. **encapsulation** *type*
12. **ipv6 enable**
13. Do one of the following:
    - **ip address negotiated**

- **ipv6 address autoconfig**
- **ipv6 dhcp client pd** *prefix-name*

14. **mtu** *size*
15. **ppp authentication pap callin**
16. **ppp pap sent-username** *username* **password** *password*
17. **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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**no ip address** **Example:** `Device(config-if)# no ip address`	Removes the IP address.
Step 5	**pppoe enable group global** **Example:** `Device(config-if)# pppoe enable group global`	Enables a PPPoE session on the Gigabit Ethernet interface.
Step 6	**pppoe-client dial-pool-number** *number* **Example:** `Device(config-if)# pppoe-client dial-pool-number 1`	Configures a PPPoE client and specifies dial-on-demand routing (DDR) functionality.
Step 7	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Removes the IP address.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**interface dialer** *number* **Example:** `Device(config)# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.

	Command or Action	Purpose
Step 10	**dialer** *pool number* **Example:** `Device(config-if)# dialer pool 1`	Specifies the dialing pool that the dialer interface uses to connect to a specific destination subnetwork.
Step 11	**encapsulation** *type* **Example:** `Device(config-if)# encapsulation ppp`	Specifies the encapsulation type. • Sets PPP as the encapsulation type.
Step 12	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on the dialer interface.

Step 13	Do one of the following:
	• **ip address negotiated**
	• **ipv6 address autoconfig**
	• **ipv6 dhcp client pd** *prefix-name*
	Example:
	For IPv4
	`Device(config-if)# ip address negotiated`
	Example:
	For IPv6
	`Device(config-if)# ipv6 address autoconfig`
	Example:
	For DHCP IPv6
	`Device(config-if)# ipv6 dhcp client pd pd1`
		Specifies how the IP address is obtained for the dialer interface. This can be through one of the following as specified:
		• PPP/IP Control Protocol (IPCP) address negotiation
		• Dynamic Host Configuration Protocol (DHCP)

Step 14	**mtu** *size* **Example:** `Device(config-if)# mtu 1492`	Sets the maximum transmission unit (MTU) size.
Step 15	**ppp authentication pap callin** **Example:** `Device(config-if)# ppp authentication pap callin`	Enables at least one PPP authentication protocol and specifies the order in which protocols are selected on the interface.
Step 16	**ppp pap sent-username** *username* **password** *password* **Example:** `Device(config-if)# ppp pap sent-username username1 password password1`	Reenables remote Password Authentication Protocol (PAP) support for an interface and reuses the username and password parameters in the PAP authentication packet to the peer.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring PPPoE on the Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *username* **password** *password*
4. **bba-group pppoe** *bba-group-name*
5. **virtual-template** *template-number*
6. **exit**
7. **interface loopback** *interface-number*
8. Do one of the following:
   - **ip address** *ip-address mask*
   - **ipv6 address** *ipv6-address /prefix*
9. **exit**
10. **interface** *type number*
11. Do one of the following:
    - **no ip address**
    - **no ipv6 address**
12. **pppoe enable group** *bba-group-name*
13. **exit**
14. **interface virtual-template** *number*
15. Do one of the following:
    - **ip unnumbered loopback** *number*
    - **ipv6 unnumbered loopback** *number*
16. **description** *description*
17. **mtu** *size*
18. Do one of the following:
    - **peer default ip address pool** *local-pool-name*
    - **peer default ipv6 address pool** *local-pool-name*
    - **ipv6 dhcp server** *dhcp-pool-name*
19. **ppp authentication** *protocol*
20. **exit**
21. **ipv6 dhcp pool** *dhcp-pool-name*
22. **prefix-delegation pool** *local-pool-name*
23. Do one of the following:
    - **ip local pool** *pool-name* [*low-ip-address* [*high-ip-address*]]
    - **ipv6 local pool** *pool-name ipv6-subnet-id /prefix prefix-length*
24. **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	**username** *username* **password** *password* **Example:** `Device(config)# username username1 password password1`	Creates a PPPoE profile and enters BBA group configuration mode.
Step 4	**bba-group pppoe** *bba-group-name* **Example:** `Device(config)# bba-group pppoe bba1`	Creates a PPPoE profile and enters BBA group configuration mode.
Step 5	**virtual-template** *template-number* **Example:** `Device(config-bba-group)# virtual-template 1`	Creates a virtual template for a PPPoE profile with an identifying number to be used for cloning virtual access interfaces. • The range is 1 to 4095.
Step 6	**exit** **Example:** `Device(config-bba-group)# exit`	Exits BBA group configuration mode and returns to global configuration mode.
Step 7	**interface loopback** *interface-number* **Example:** `Device(config)# interface loopback 1`	Creates a loopback interface that emulates an interface that is always up and enters interface configuration mode. • The range is from 0 to 2147483647.

Step 8	Do one of the following:
	• **ip address** *ip-address mask*
	• **ipv6 address** *ipv6-address /prefix*
	Example:
	Using an IPv4 address:
	`Device(config-if)# ip address 192.2.0.2 255.255.255.0`
	Example:
	Using an IPv6 address:
	`Device(config-if)# ipv6 address 2001:DB8:2::1/40`
		Assigns an IP address to the loopback interface.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Configures an interface and enters interface configuration mode.

Step 11	Do one of the following:
	• **no ip address**
	• **no ipv6 address**
	Example:
	For an IPv4 address:
	`Device(config-if)# no ip address`
	Example:
	For an IPv6 address:
	`Device(config-if)# no ipv6 address`
		Removes the IP address.

Step 12	**pppoe enable group** *bba-group-name* **Example:** `Device(config-if)# pppoe enable group bba1`	Enables PPPoE sessions on the Gigabit Ethernet interface.
Step 13	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 14	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically to create virtual access interfaces and enters interface configuration mode.

Step 15	Do one of the following:
	• **ip unnumbered loopback** *number*
	• **ipv6 unnumbered loopback** *number*
	Example:
	For IPv4:
	`Device(config-if)# ip unnumbered loopback 1`
	Example:
	For IPv6:
	`Device(config-if)# ipv6 unnumbered loopback 1`
		Enables IP processing on an interface without explicitly assigning an IP address to the interface.
		• The *type* argument is the interface on which the router has assigned an IP address.
		• The *number* argument is the number of the interface on which you want to enable IP processing.

	Command or Action	Purpose
Step 16	**description** *description* **Example:** `Device(config-if)# description pppoe bba1`	Adds a description to an interface configuration
Step 17	**mtu** *size* **Example:** `Device(config-if)# mtu 1492`	Sets the MTU size. • The range is from 64 to 9216.

Step 18	Do one of the following:
	• **peer default ip address pool** *local-pool-name*
	• **peer default ipv6 address pool** *local-pool-name*
	• **ipv6 dhcp server** *dhcp-pool-name*
	Example:
	For IPv4 addresses
	`Device(config-if)# peer default ip address pool pool1`
	Example:
	For IPv6 addresses
	`Device(config-if)# peer default ipv6 address pool pool1`
	Example:
	For DHCP assigned addresses:
	`Device(config-if)# ipv6 dhcp server dhcpv6pool`
		Specifies an address pool to provide IP addresses for remote peers connecting to this interface.

Step 19	**ppp authentication** *protocol* **Example:** `Device(config-if)# ppp authentication pap`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 21	**ipv6 dhcp pool** *dhcp-pool-name* **Example:** `Device(config)# ipv6 dhcp pool dhcpv6pool`	Creates a DHCP information pool and configures a local prefix pool from which prefixes can be delegated to clients.
Step 22	**prefix-delegation pool** *local-pool-name* **Example:** `Device(config-dhcpv6)# prefix-delegation pool pool1`	Specifies a local prefix pool.

	Command or Action	Purpose

Step 23	Do one of the following:
	• **ip local pool** *pool-name* [*low-ip-address* [*high-ip-address*]]
	• **ipv6 local pool** *pool-name ipv6-subnet-id /prefix prefix-length*
	Example:
	For IPv4 addresses
	`Device(config)# ip local pool pool1 192.2.0.1 192.2.0.10`
	Example:
	For IPv6 addresses
	`Device(config)# ipv6 local pool pool1 2001:DB8:1200::/40 48`
		Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

Step 24	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a PPPoE Client over a VLAN Interface

Perform this task to configure a PPPoE client over a VLAN interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **switchport trunk allowed vlan** *vlan-list*
5. **switchport mode** {*access* | *trunk*}
6. **end**
7. **interface** *type number*
8. **no ip address**
9. **pppoe enable group global**
10. **pppoe-client dial-pool-number** *number*
11. **end**
12. **interface** *type number*
13. **ip address negotiated**
14. **encapsulation** *encapsulation-type*
15. **dialer pool** *number*
16. **pppoe pap sent-username** *username* **password** *password*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**switchport trunk allowed vlan** *vlan-list* **Example:** `Device(config-if)# switchport trunk allowed vlan 10`	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
Step 5	**switchport mode** {*access* | *trunk*} **Example:** `Device(config-if)# switchport mode trunk`	Enables switchport mode. To specify a trunking VLAN interface, use the **switchport mode trunk** command.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface vlan 10`	Configures an interface and enters interface configuration mode.
Step 8	**no ip address** **Example:** `Device(config-if)# no ip address`	Disables IP processing for an interface.
Step 9	**pppoe enable group global** **Example:** `Device(config-if)# pppoe enable group global`	Enables a PPPoE session on the Gigabit Ethernet interface.
Step 10	**pppoe-client dial-pool-number** *number* **Example:** `Device(config-if)# pppoe-client dial-pool-number 2`	Configures a PPPoE client and specifies dial-on-demand routing (DDR) functionality.
Step 11	**end** **Example:**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 12	**interface** *type number* **Example:** `Device(config)# interface Dialer2`	Configures an interface and enters interface configuration mode.
Step 13	**ip address negotiated** **Example:** `Device(config-if)# ip address negotiated`	Specifies that the IP address for the interface is obtained through PPP or IPCP (IP Control Protocol) address negotiation.
Step 14	**encapsulation** *encapsulation-type* **Example:** `Device(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface. To set PPP as the encapsulation type, use the **encapsulation ppp** command.
Step 15	**dialer pool** *number* **Example:** `Device(config-if)# dialer pool 2`	Specifies the dialing pool for a dialer interface to connect to a specific destination subnetwork.
Step 16	**pppoe pap sent-username** *username* **password** *password* **Example:** `Device(config-if)# ppp pap sent-username cisco@cisco.com password cisco`	Enables remote PAP support for an interface and authenticates the request packet to the peer.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying a PPPoE Client over a VLAN Interface

To verify that the PPPoE session is established, run the **show pppoe session** command. You should see the state type as UP.

```
ovld1# show pppoe session

     1 client session

Uniq ID  PPPoE  RemMAC          Port               VT   VA         State
           SID  LocMAC                                  VA-st      Type
    N/A    1    0000.aaaa.bbb0  V110               Di2  Vi2        UP
                0101.xxx1.dccc                          UP
```

Configuration Examples for the PPP over Ethernet Client

Example: Configuring a PPPoE Client

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# pppoe enable
Device(config-if)# pppoe-client dial-pool-number 1
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface dialer 1
Device(config-if)# mtu 1492
Device(config-if)# ip address negotiated
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# ppp pap sent-username username1 password password1
Device(config-if)# end
```

Example: Configuring PPPoE on IPv4

Example: Server Configuration

```
Device> enable
Device# configure terminal
Device# username username1 password password1
Device(config)# bba-group pppoe bba1
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# exit
Device(config)# interface loopback 1
Device(config-if)# ip address 192.2.0.2 255.255.255.0
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# negotiation auto
Device(config-if)# pppoe enable group bba1
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface virtual-template 1
Device(config-if)# description pppoe bba1
Device(config-if)# mtu 1492
Device(config-if)# ip unnumbered loopback 1
Device(config-if)# peer default ip address pool pool1
Device(config-if)# ppp authentication pap
Device(config-if)# exit
Device(config)# ip local pool pool1 192.2.0.1 192.2.0.10
Device(config)# end
```

Example: Client Configuration

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# pppoe enable
Device(config-if)# pppoe-client dial-pool-number 1
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface dialer 1
Device(config-if)# mtu 1492
Device(config-if)# ip address negotiated
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# ppp pap sent-username username1 password password1
Device(config-if)# end
```

Example: Configuring PPPoE on IPv6 using DHCP

Example: Server Configuration using DHCP

Configure a username and a password for PPP client:

```
Host(config)# username username1 password password1
```

Create a PPP group GROUPA and associate it with a Virtual Template 1:

```
Host(config)# bba-group pppoe GROUPA
Host(config-bba-group)# virtual-template 1
Host(config-bba-group)# exit
```

Configure a loopback interface to be used on the Virtual Template 1:

```
Host(config)# interface loopback 1
Host(config-if)# ipv6 address 2001:DB8:2::1/40

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Host(config-if)# exit
```

Create a Virtual Template 1 and use the loopback interface as the IP address:

```
Host(config)# interface virtual-template 1
Host(config-if)# ipv6 unnumbered loopback 1
Host(config-if)# description pppoe GROUPA
Host(config-if)# mtu 1492

!Specify that PPP PAP authentication is used for authenticating connecting PPP
!clients
Host(config-if)# ppp authentication pap

!Enables DHCP for IPv6 service for the interface and specifies a pool for prefix
!delegation.
Host(config-if)# ipv6 dhcp server dhcpv6pool

Host(config-dhcp)# exit
```

Associate a physical interface with the PPP group GROUPA:

```
Host(config)# interface FastEthernet 0/0
Host(config-if)# no ip address
Host(config-if)# pppoe enable group GROUPA
Host(config-if)# no shutdown
Host(config-if)# exit
```

Create the local IPV6 address pool pool1 referred to in the Virtual Template 1

```
Host(config)# ipv6 local pool pool1 2001:DB8:1200::/40 48
```

Create a DHCP information pool and configure a local prefix pool from which prefixes can be delegated to clients.

```
Host(config)# ipv6 dhcp pool dhcpv6pool

!Specify local prefix pool
Host(config-dhcpv6)# prefix-delegation pool pool1
Host(config-dhcpv6)# end
```

Example: Client Configuration using DHCP

```
Device> enable
Device# configure terminal
Device(config)# hostname Client
```

Configure a physical interface and allocate it to a dialer pool. A logical dialer interface associated with the dialer pool can select a physical interface from this dialer pool when needed.

```
Client(config)# interface FastEthernet 0/0
Client(config-if)# no ip address
Client(config-if)# pppoe enable group global

!Allocate the physical interface to the dialer pool
Client(config-if)# pppoe-client dial-pool-number 1
Client(config-if)# no shutdown

%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Client(config-if)# exit
```

Create the logical dialer interface and configure the pool used to pick physical interfaces

```
Client(config)# interface dialer 1

!Configure the pool used to pick physical interfaces.
Client(config-if)# dialer pool 1

!Sets the encapsulation method used by the interface to PPP.
Client(config-if)# encapsulation ppp
Client(config-if)# ipv6 enable

*Jun  2 23:51:36.455: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jun  2 23:51:36.459: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jun  2 23:51:36.507: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Jun  2 23:51:36.519: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down

!Enable Prefix delegation on the interface
Client(config-if)# ipv6 dhcp client pd dhcp_prefix_label

!Reduce MTU of the dialer interface to avoid unnecessary fragmentation caused by added
```

```
PPP headers.
Client(config-if)# mtu 1492
Client(config-if)# ppp authentication pap callin

!Configures the username and password that the client can use to authenticate with the
 server.
Client(config-if)# ppp pap sent-username username1 password password1

*Jun  2 23:52:20.999: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jun  2 23:52:21.003: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jun  2 23:52:21.103: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
Client(config-if)# end
```

Example: Verifying the PPPoE connection

Observe the interfaces of the client:

```
Client#show ipv6 interface brief

FastEthernet0/0            [up/up]
    unassigned
Dialer1                    [up/up]
    FE80::205:FF:FE50:6C08
Virtual-Access1            [up/up]
    unassigned
```

Observe the PPPoE session on the client:

```
Client# show pppoe session

     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    324  0005.0050.9c08  Fa0/0                  Di1  Vi2        UP
                0005.0050.6c08                              UP
```

Observe the packets exchanged during the PPPoE session:

```
Client# show pppoe session packets

Total PPPoE sessions 1

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
2846    0               6216            0               128136
```

Observe the DHCP session:

```
Server# show ipv6 dhcp binding

Client: FE80::205:FF:FE50:6C08
  DUID: 00030001000500506C08
  Username : unassigned
  Interface : Virtual-Access1.1
  IA PD: IA ID 0x000D0001, T1 302400, T2 483840
    Prefix: 2001:DB8::/48
            preferred lifetime 604800, valid lifetime 2592000
            expires at Jul 01 2013 09:17 PM (2591979 seconds)

Server# show ipv6 dhcp pool
```

```
DHCPv6 pool: dhcpv6pool
  Prefix pool: pool1
               preferred lifetime 604800, valid lifetime 2592000
  Active clients: 1
```

Example: Configuring PPPoE on IPv6

Configuring PPPoE on the Server

```
Device> enable
Device# configure terminal
Device(config)# hostname Host
```

Configure a username and a password for PPP client:

```
Host# username username1 password password1
```

Create a PPP group GROUPA and associate it with a Virtual Template 1:

```
Host(config)# bba-group pppoe GROUPA

*Jun  1 21:30:55.587: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Jun  1 21:30:55.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
Host(config-bba-group)# virtual-template 1
Host(config-bba-group)# exit
```

Configure a loopback interface to be used on the Virtual Template 1:

```
Host(config)# interface loopback 1
Host(config-if)# ipv6 address 2001:DB8:2::1/40

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
Host(config-if)# exit
```

Create a Virtual Template 1 and use the loopback interface as the IP address:

```
Host(config)# interface virtual-template 1
Host(config-if)# ipv6 unnumbered loopback 1
Host(config-if)# description pppoe GROUPA
Host(config-if)# mtu 1492

!Configure the Virtual Template to hand out IP addresses from pool1
Host(config-if)# peer default ipv6 pool pool1

!Specify that PPP PAP authentication is used for authenticating connecting PPP clients
Host(config-if)# ppp authentication pap
Host(config-if)# exit
```

Associate a physical interface with the PPP group GROUPA:

```
Host(config)# interface FastEthernet 0/0
Host(config-if)# no ip address
Host(config-if)# pppoe enable group GROUPA
Host(config-if)# no shutdown
Host(config-if)# exit

*Jun  1 21:33:07.199: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun  1 21:33:08.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

Create the IPV6 address pool pool1 referred to in the Virtual Template 1:

```
Host(config)# ipv6 local pool pool1 2001:DB8:1200::/40 48
Host(config)# end
```

Configuring PPPoE on the Client

```
Device> enable
Device# configure terminal
Device(config)# hostname Host
```

Configure a physical interface and allocate it to a dialer pool. A logical dialer interface associated with the dialer pool can select a physical interface from this dialer pool when needed.

```
Client(config)# interface FastEthernet 0/0
Client(config-if)# no ip address
Client(config-if)# pppoe enable group global

!Allocate the physical interface to the dialer pool
Client(config-if)# pppoe-client dial-pool-number 1
Client(config-if)# no shutdown

%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
Client(config-if)# exit
```

Create the logical dialer interface and configure the pool used to pick physical interfaces

```
Client(config)# interface dialer 1

!Configure the pool used to pick physical interfaces.
Client(config-if)# dialer pool 1

!Sets the encapsulation method used by the interface to PPP.
Client(config-if)# encapsulation ppp
Client(config-if)# ipv6 enable

*Jun  3 00:10:48.031: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jun  3 00:10:48.035: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jun  3 00:10:48.083: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Jun  3 00:10:48.091: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down

!Configure the PPP clients to get IP addresses for dialer interfaces by using
!PPP negotiations with the server.
Client(config-if)# ipv6 address autoconfig

!Reduce MTU of the dialer interface to avoid unnecessary fragmentation caused by added PPP

!headers
Client(config-if)# mtu 1492
Client(config-if)# ppp authentication pap callin

!Configures the username and password that the client can use to authenticate with the
!server.
Client(config-if)# ppp pap sent-username username1 password password1

*Jun  3 00:11:54.843: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jun  3 00:11:54.847: %LINK-3-UPDOWN: Interface Virtual-Access2, changed
 state to up
*Jun  3 00:11:54.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

```
Virtual-Access2, changed state to up

Client(config-if)# end
```

Verifying the PPPoE connection

Observe the interfaces of the client:

```
Client# show ipv6 interface brief

FastEthernet0/0            [up/up]
    unassigned
Dialer1                    [up/up]
    FE80::205:FF:FE50:6C08
Virtual-Access1            [up/up]
    unassigned
```

Observe the PPPoE session on the client:

```
Client# show pppoe session

     1 client session

Uniq ID  PPPoE  RemMAC          Port                  VT  VA         State
           SID  LocMAC                                    VA-st      Type
    N/A    324  0005.0050.9c08  Fa0/0                 Di1  Vi2        UP
                0005.0050.6c08                             UP
```

Observe the packets exchanged during the PPPoE session:

```
Client# show pppoe session packets

Total PPPoE sessions 1

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
2846    0               6216            0               128136
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband Access Aggregation and DSL commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

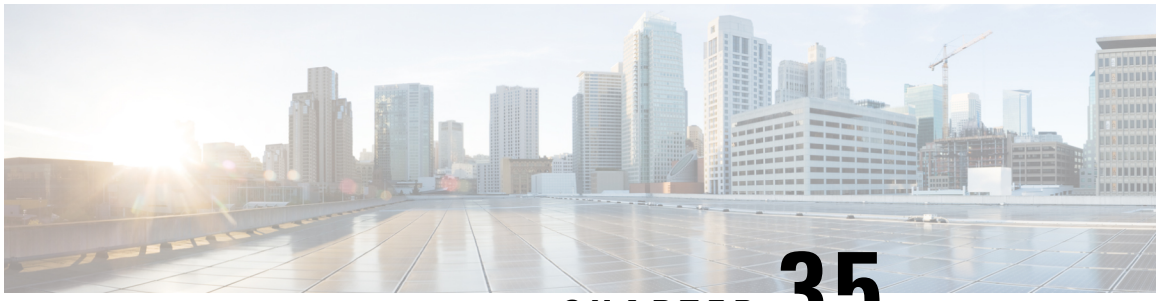
Feature Information for PPP over Ethernet Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 41: Feature Information for PPP over Ethernet Client

Feature Name	Releases	Feature Information
PPP over Ethernet Client for IPv6	Cisco IOS XE Release 3.9S	The PPP over Ethernet Client feature provides IPv6 support.
PPP over Ethernet Client	Cisco IOS XE Release 3.5S	This feature was introduced. The PPP over Ethernet Client feature provides PPPoE client support on routers.
PPPoE Client over VLAN Interface	Cisco IOS XE Release Bengaluru 17.6	This feature was introduced. The PPPoE Client over VLAN Interface feature allows users to establish a PPPoE session over a VLAN interface.



CHAPTER 35

VRF Awareness Access Class Line

The VRF Awareness Access Class Line feature supports access-class command on the VTY line for IPv4 and IPv6.

Feature Information for VRF Awareness Access Class Line

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 42: Feature Information for VRF Awareness Access Class Line

Feature Name	Releases	Feature Information
VRF Awareness Access Class Line	Cisco IOS XE Release 16.8.1	The VRF Awareness Access Class Line feature supports access-class command on the VTY line for IPv4 and IPv6. The following commands were introduced or modified by this feature: **access-class** *acl-name* **in** *vrfname* **vrf**, **ipv6 access-class** *acl-name* **in***vrfname* **vrf**.

Restrictions for VRF Awareness Access-Class Line

- The **vrf-also** keyword is mutually exclusive of **access-class line** command.
- Multiple VRFs cannot be configured on a single **access-class line** command. For example:

```
line vty 0 4
access-class acl1 in vrfA vrfB vrfc >>>is not supported
```

- When the **vrf aware access-class line** command for the same VRF is re-configured, the last configuration replaces the earlier one.
- If the **access-class line** command is configured with multiple VRFs (for example, vrfA, vrfB, vrfC) on a VTY line and the traffic passes through a different VRF (for example, vrfD), then the packets are dropped.
- There is only one vrf aware **access-class line** command for one VRF. For example:

```
Line vty 0 4
Access-class acl-1 in vrfname vrfA
Access-class acl-2 in vrfname vrfB
Access-class acl-1 in vrfname vrfC
```

Information About VRF Awareness Access Class Line

VRF Awareness Access Class Line

You can control the accessibility of the virtual terminal lines (VTY) to a device by applying an access list to inbound VTYs. You can also control the destinations that the VTYs from a device can reach by applying an access list to outbound VTYs.

Note When you apply an access list to a VTY using the **access-class** command, the access list can be a numbered access list or a named access list.

How to Configure VRF Awareness Access Class Line

Configure Access-Class on the VTY line

To configure the **access-class** command on the VTY line for IPv6, identify a specific line for configuration. Enter the line command with the optional line type VTY, which is the line number.

```
Device(config)# line vty 0 4
Device(config-line)# ipv6 access-class acl-name in vrfname vfrA
```

Note You also can use the **line** command without specifying a line type. In this case, the line number is treated as an absolute line number.

Configure Multiple Routing Tables or VRFs using Access-Class

To configure multiple routing tables or VRFs:

```
Device(config)# line vty 0 4
Device(config-line)# ipv6 access-class acl-1 in vrf vrfA
Device(config-line)# ipv6 access-class acl-2 in vrf vrfB
Device(config-line)# ipv6 access-class acl-1 in vrf vrfC
```

Configuration Examples for VRF Awareness Access Class Line

Example: VRF Awareness Access-Class for IPv4 and IPv6

```
line vty 0 4
access-class acl-1 in vrfname vrfA
```

```
line vty 0 5
ipv6 access-class acl-1 in vrfname MGMT
ipv6 access-class acl-2 in vrfname LOOP
```

Additional References for VRF Awareness Access Class Line

Related Documents

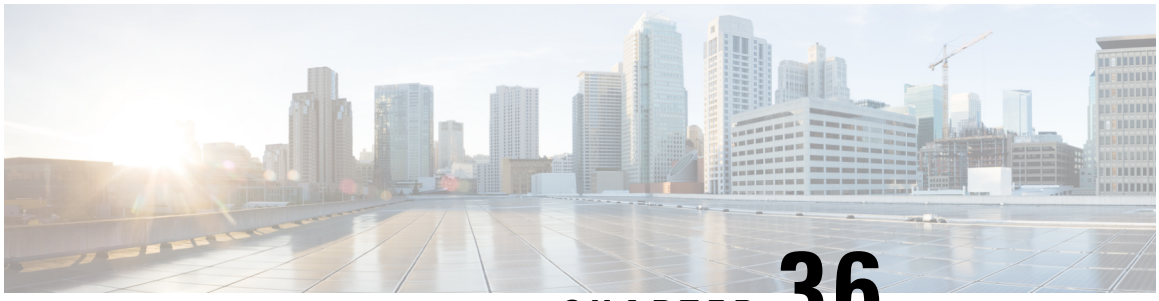
Related Topic	Document Title

MIBs

MIB	MIBs Link
• CISCO-VRF-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 36

PPPoE Smart Server Selection

The PPPoE Smart Server Selection feature allows service providers to determine which Broadband Remote Access Server (BRAS) a PPP call will terminate on.

The PPPoE Smart Server Selection feature allows you to configure a specific PPP over Ethernet (PPPoE) Active Discovery Offer (PADO) delay for a received PPPoE Active Discovery Initiation (PADI) packet. The PADO delay establishes the order in which the BRASs respond to PADIs by delaying their responses to particular PADIs by various times.

Information About PPPoE Smart Server Selection

Benefits of PPPoE Smart Server Selection

PPPoE Smart Server Selection provides the following benefits for the Internet service providers (ISPs):

- Optimize their networks by predicting and isolating PPP calls to terminate on a particular BRAS.
- Establish a priority order among the BRASs by configuring varying degrees of delays in the broadband access (BBA) groups on different BRASs.
- Use circuit ID and remote ID tag matching with strings up to 64 characters in length.
- Use spaces in remote ID, circuit ID, and PPPoE service names.
- Restrict the service advertisements from a BRASs in a PADO message.
- Apply a PADO transmission delay based on circuit ID, remote ID, and service name.
- Do partial matching on service name, remote ID, and circuit ID.

How to Configure PPPoE Smart Server Selection

Configuring BBA Group PADO Delay

Perform this task to allow all calls coming into a defined BBA group on a Broadband Remote Access Server (BRAS) to be treated with the same priority. All incoming sessions for a particular group would have their PADO responses delayed by the configured number of milliseconds.

This task allows Internet Service Providers (ISPs) to establish a priority order among the BRASs by configuring varying degrees of delays in the BBA groups on different BRASs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **pado delay** *milliseconds*

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	**bba-group pppoe** {*group-name* | **global**} **Example:** `Device(config)# bba-group pppoe server-selection`	Defines a PPP over Ethernet (PPPoE) profile, and enters BBA group configuration mode. • The **global** keyword creates a profile, which serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**pado delay** *milliseconds* **Example:** `Device(config-bba-group)# pado delay 512`	Sets the time by which a PADO response is delayed for a BBA group. **Note** The value assigned for milliseconds should be a multiple of 256. Even though the device allows other values, the Cisco Software rounds the values down to the closest multiple of 256.

Troubleshooting Tips

Use the **debug pppoe** command to troubleshoot the PPPoE session.

Configuring PADO Delay Based on Remote ID or Circuit ID

This task uses the **pppoe server** command to define a list of circuit ID and remote ID tags on a BRAS for a particular BBA group. The **pppoe delay** command is extended to specify delays based on the PPPoE circuit ID or remote ID tag.

All incoming calls are scanned and if the circuit ID or remote ID tags in the PADI match the list on the BRAS, then the PADO response will be delayed by the configured delay time. If there is no delay defined based on the circuit ID or remote ID, the per-PPPoE service delay is sought. It it is not found, the delay for the BBA group PADO is used. If no PPPoE delay is found, the PADO is sent without delay.

If there is no match and a BBA group PADO delay is configured under the same BBA group, then the PADO response is delayed by the configured delay time for that BBA group. If a BBA group PADO delay is not configured, then the PADO response is sent immediately.

With PPPoE smart server selection, you can do a partial match for a configured string by using a circuit ID or remote ID delay configured for the PPPoE server. (*Partial matching* is searching for parts of strings. It is used to search for similar strings.)

Perform this task to define a list of circuit ID and remote ID tags on a BRAS for a particular BBA group and configures the delay associated with the circuit ID and remote ID tags.

Note The value assigned for milliseconds should be a multiple of 256. Even though the device allows other values, the Cisco Software rounds the values down to the closest multiple of 256.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **pppoe server circuit-id delay** *milliseconds* **string** [**contains**] *circuit-id-string*
5. **pppoe server remote-id delay** *milliseconds* **string** [**contains**] *remote-id-string*
6. **pado delay circuit-id** *milliseconds*
7. **pado delay remote-id** *milliseconds*
8. **pado delay** *milliseconds*
9. **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	**bba-group pppoe** {*group-name* | **global**} **Example:** `Device(config)# bba-group pppoe server-selection`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port.
Step 4	**pppoe server circuit-id delay** *milliseconds* **string** [**contains**] *circuit-id-string* **Example:** `Device(config-bba-group)# pppoe server circuit-id delay 256 string circuit ATM1/0/0 VC 0/100`	(Optional) Specifies the delay to be applied based on the PPPoE tag circuit ID from the client. • The **contains** keyword can find a partial match for this delay statement. • The value for the *circuit-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, "circuit ATM1/0/0 VC 0/100").
Step 5	**pppoe server remote-id delay** *milliseconds* **string** [**contains**] *remote-id-string* **Example:** `Device(config-bba-group)# pppoe server remote-id delay 512 string XTH-TEST`	(Optional) Specifies the delay to be applied based on the PPPoE tag remote ID from the client. • The **contains** keyword can find a partial match for this delay statement. • The value for the *remote-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, "subscr mac 1111.2222.3333").
Step 6	**pado delay circuit-id** *milliseconds* **Example:** `Device(config-bba-group)# pado delay circuit-id 768`	(Optional) Finds a match based on the PPPoE group circuit ID delay if configured.. • If a circuit ID cannot be matched partially, a delay is applied based on any circuit ID that is present.
Step 7	**pado delay remote-id** *milliseconds* **Example:** `Device(config-bba-group)# pado delay remote-id 256`	(Optional) Finds a match based on the PPPoE group remote ID delay if configured..
Step 8	**pado delay** *milliseconds* **Example:** `Device(config-bba-group)# pado delay 512`	(Optional) Uses the group PADO delay configuration. Sets the time by which a PADO response is delayed for a BBA group. • The PADO delay value is sought if the PADO delay is not found after several attempts.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug pppoe event** command to verify the smart server PADO delay selection.

Configuring PPPoE Service PADO Delay

Perform this task to specify a delay based on the PPPoE service. A delay is applied to the PADO offering based on the service name match.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policymap-name*
4. **exit**
5. **bba-group pppoe** [**global** | *profile-name*]
6. **virtual-template** *interface-number*
7. **service profile** *subscriber-profile-name* **refresh** *minutes*
8. **service name match**
9. **pado delay** *milliseconds*
10. **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	**policy-map type service** *policymap-name* **Example:** `Device(config)# policy-map type service serv3`	Places the device in service policy map configuration mode, and defines the name of service policy map.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-service-policymap)# exit`	Exits service policy map configuration mode and returns to global configuration mode.
Step 5	**bba-group pppoe** [**global** | *profile-name*] **Example:** `Device(config-bba-group)# bba-group pppoe global`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port.
Step 6	**virtual-template** *interface-number* **Example:** `Device(config-bba-group)# virtual-template 20`	Specifies the virtual template interface number for the BBA group, and places the device in configuration BBA group mode.
Step 7	**service profile** *subscriber-profile-name* **refresh** *minutes* **Example:** `Device(config-bba-group)# service profile serv3 refresh 30`	Specifies the subscriber profile to be associated with the BBA group, and the refresh interval minutes for the service profile.
Step 8	**service name match** **Example:** `Device(config-bba-group)# service name match`	Matches the requested tag for the PPPoE global group. **Note** The **service name match** command must be configured per the PPPoE service delay. The requested service by the client should also be configured on the BRAS to ensure PADO response from the BRAS.
Step 9	**pado delay** *milliseconds* **Example:** `Device(config-bba-group)# pado delay 512`	(Optional) Uses the group PADO delay configuration. Sets the time by which a PADO response is delayed for a BBA group. • The PADO delay value is sought if the PADO delay is not found after several attempts. **Note** The value assigned for milliseconds should be a multiple of 256. Even though the device allows other values, the Cisco Software rounds the values down to the closest multiple of 256.
Step 10	**end** **Example:** `Device(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug pppoe event**command to verify the service name match and PADO delay for a PPPoE service.

Configuration Examples for PPPoE Smart Server Selection

Configuring BBA Group PADO Delay Example

The following example shows how to configure a BBA group for PADO delay:

```
Device> enable
Device# configure terminal
Device(config)# bba-group pppoe server-selection
Device(config-bba-group)# pado delay 512
Device(config-bba-group)# end
```

Configuring PADO Delay Example

The following example shows how to match the string by using a circuit ID or remote ID delay configured for PPPoE server:

```
Device> enable
Device# configure terminal
Device(config)# bba-group pppoe server-selection
Device(config-bba-group)# pppoe server circuit-id delay 256 string "subscr mac 1111.2222.3333"
Device(config-bba-group)# pado delay circuit-id 512
Device(config-bba-group)# pado delay remote-id 768
Device(config-bba-group)# end
```

The following example shows how to configure PADO delay based on the remote ID or circuit ID:

```
Device> enable
Device# configure terminal
Device(config)# bba-group pppoe server-selection
Device(config-bba-group)# pppoe server remote-id delay 512 string contains TEST
Device(config-bba-group)# pppoe server remote-id delay 256 string XTH
Device(config-bba-group)# pppoe server remote-id delay 768 string contains XTH-TEST
Device(config-bba-group)# end
```

Generally, the first match found in the list is considered for the delay value. If the remote ID in the client PPPoE tag contains XTH-TEST, then the delay value is 512. In this case, the first match succeeds and the configuration never reaches a delay of 768. If the remote ID in the client PPPoE tag contains TH- no, then no match is found.

Configuring PPPoE Service PADO Delay Example

The following example shows how to configure the PADO delay based on the PPPoE service:

```
Device> enable
Device# configure terminal
```

```
Device(config)# policy-map type service XTH-services
Device(config-service-policymap)# pppoe service ILoBr delay 768
Device(config-service-policymap)# pppoe service xth-service1 delay 256
Device(config-service-policymap)# pppoe service service-nodelay
Device(config-service-policymap)# exit
Device(config)# bba-group pppoe server-selection
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# service svc-group
Device(config-bba-group)# service profile XTH-services
Device(config-bba-group)# service name match
Device(config-bba-group)# pado delay 512
Device(config-bba-group)# end
```

Verifying the PPPoE Service Match and PADO Delay Example

The following example shows the output of the service name match and PADO delay for a PPPoE service using the **show pppoe derived group** *group-name* command. This command prints all the PPPoE services for the supported groups and also shows the associated delay for this service.

```
Device# show pppoe derived group svc-group

Derived configuration from subscriber profile 'XTH-services':
Service names: servicename:pado-delay
ILoBr:768, xth-service1:256, service nodelay:0
```

Additional References

The following sections provide references related to the PPPoE Smart Server Selection feature.

Related Documents

Related Topic	Document Title
Configuring broadband and DSL	*Cisco IOS XE Broadband and DSL Configuration Guide*
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* •

Standards

Standard	Title
None	-

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

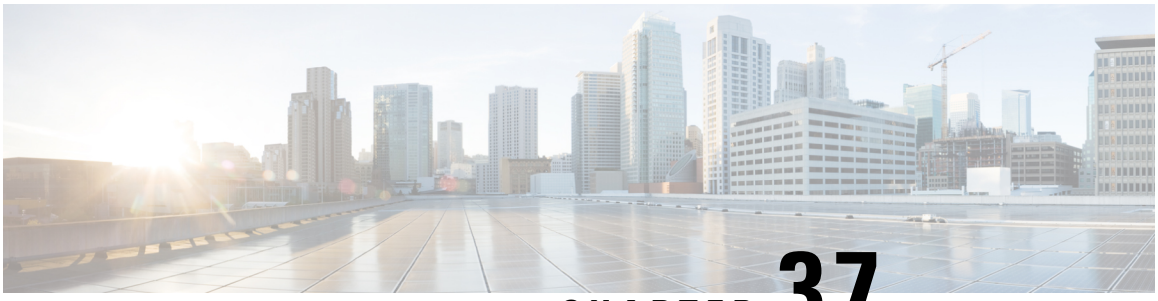
Feature Information for PPPoE Smart Server Selection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 43: Feature Information for PPPoE Smart Server Selection

Feature Name	Releases	Feature Information
PPPoE Smart Server Selection	Cisco IOS XE Release 2.4	PPPoE Smart Server Selection allows service providers to determine which Broadband Remote Access Server (BRAS) a PPP call will terminate on.



CHAPTER 37

Monitoring PPPoE Sessions with SNMP

The PPPoE Session Count Management Information Base feature provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPP over Ethernet (PPPoE) sessions configured on permanent virtual circuits (PVCs) and on a router.

The SNMP Traps for PPPoE Session Limits feature provides SNMP MIB support for the PPPoE session limits and generates notifications in case the limits are reached.

This MIB also supports two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router. The PPPoE session-count thresholds can be configured using the **sessions max limit** and **pppoe max-sessions** commands.

Prerequisites for Monitoring PPPoE Sessions with SNMP

- You must understand the concepts described in the Preparing for Broadband Access Aggregation module.
- PPPoE sessions must be established using the procedures in the Providing Protocol Support for Broadband Access Aggregation of PPPoE Session s module.

Restrictions for Monitoring PPPoE Sessions with SNMP

The **snmp-server enable traps pppoe** command enables SNMP traps only. It does not support inform requests.

Information About Monitoring PPPoE Sessions with SNMP

Network Management Protocol

SNMP is a network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security. SNMP version 2 supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

PPPoE Session Count MIB

A MIB is a database of network management information that is used and maintained by a network management protocol, such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system.

The PPPoE Session Count MIB uses two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router. The PPPoE session-count thresholds can be configured using the **sessions max limit** and **pppoe max-sessions** commands. You can also set per-MAC session and IWF limits for a PPPoE session, per-MAC throttle rate limit for a PPPoE session, per-VLAN session configuration limit, per-VLAN throttle rate limit, per-VC session configuration limit, and per-VC throttle rate limit configuration limit.

The table below describes the objects and tables supported by the PPPoE Session-Count MIB. For a complete description of the MIB, see the PPPoE Sessions Management MIB file CISCO-PPPOE-MIB.my, available through Cisco.com at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index.

Table 44: PPPoE Session Count MIB Objects and Tables

Object or Table	Description
cPppoeSystemCurrSessions	Number of PPPoE sessions active on the router.
cPppoeSystemHighWaterSessions	Highest number of PPPoE sessions configured at a particular time after the system was initialized.
cPppoeSystemMaxAllowedSessions	Number of PPPoE sessions configurable on the router.
cPppoeSystemThresholdSessions	Threshold value of PPPoE sessions configurable on the router.
cPppoeSystemExceededSessionErrors	Accumulated number of errors on the router that have occurred because the cPppoeSystemCurrSessions value exceeded the cPppoeSystemMaxAllowedSessions value.
cPppoeSystemPerMacSessionlimit	Per-MAC session limit for a PPPoE session
cPppoeSystemPerMacIWFSessionlimit	Per-MAC session IWF limit for a PPPoE session
cPppoeSystemPerMacThrottleRatelimit	Per-MAC throttle rate limit for a PPPoE session
cPppoeSystemPerVLANlimit	Per-VLAN session configuration limit

Object or Table	Description
cPppoeSystemPerVLANthrottleRatelimit	Per-VLAN throttle rate limit
cPppoeSystemPerVClimit	Per-VC session configuration limit
cPppoeSystemPerVCThrottleRatelimit	Per-VC throttle rate limit configuration limit
cPppoeVcCfgTable	PPPoE protocol-related configuration information about the virtual channel links (VCLs).
cPppoeVcSessionsTable	Configuration information and statistics about the number of PPPoE sessions on the VCLs.
cPppoeSystemSessionThresholdTrap	Generates a notification message when the number of PPPoE sessions on the router reaches the configured threshold value.
cPppoeVcSessionThresholdTrap	Generates a notification message when the number of PPPoE sessions on the PVC reaches the configured threshold value.

Benefits of Monitoring PPPoE Sessions with SNMP

The monitoring of PPPoE sessions with SNMP provides the following benefits:

- It helps manage the number of PPPoE sessions configured on a router or PVC by sending notification messages when the PPPoE session threshold has been reached.
- It provides a way of tracking PPPoE session information over time.

How to Configure Monitoring of PPPoE Sessions with SNMP

Configuring the PPPoE Session-Count Threshold for the Router

Perform this task to configure the PPPoE session-count threshold for the router.

Note The **sessions max limit** command is available only if you configure the **bba-group pppoe** command using the **global** keyword.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **bba-group pppoe** {*group-name* | **global**}
5. **sessions max limit** *session-number* [**threshold** *threshold-value*]
6. **virtual-template** *template-number*

7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE sessions have been reached.
Step 4	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode.
Step 5	**sessions max limit** *session-number* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 4000 threshold 3000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold at which an SNMP trap will be generated. **Note** This command applies only to the global profile.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template that will be used to clone the virtual access interfaces (VAI).
Step 7	**end** **Example:** `Router(config-bba-group)# end`	Exits BBA group configuration mode and returns to privileged EXEC mode.
Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a PVC

Perform this task to configure the PPPoE session-count threshold for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [*.subinterface*] [**multipoint** | **point-to-point**]
5. **pvc** [*name*] *vpi* / *vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe**
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [*.subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 5/120`	Creates an ATM PVC and enters ATM VC configuration mode.
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or

	Command or Action	Purpose
	Example: `Router(config-if-atm-vc)# pppoe max-sessions 5 threshold-sessions 3`	VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 7	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPPoE sessions to be established on ATM PVCs.
Step 8	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits ATM VC configuration mode and returns to sub interface mode.
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a VC Class

Perform this task to configure the PPPoE session-count threshold for a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **vc-class atm** *name*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **protocol pppoe** [**group** *group-name* | **global**]
7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm main`	Creates a VC class for an ATM PVC, or SVC, or ATM interface and enters VC class configuration mode.
Step 5	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-vc-class)# pppoe max-sessions 7 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-vc-class)# protocol pppoe group one`	Enables PPPoE sessions to be established.
Step 7	**end** **Example:** `Router(config-vc-class)# end`	(Optional) Exits VC class configuration mode and returns to privileged EXEC mode.
Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for an ATM PVC Range

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe** [**group** *group-name* | **global**]
8. **end**

9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [*.subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters the subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 3/100 3/105`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-range)# pppoe max-sessions 20 threshold-sessions 15`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 7	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-if-atm-range)# protocol pppoe group two`	Enables PPPoE sessions to be established.
Step 8	**end** **Example:**	(Optional) Exits ATM PVC range configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-if-atm-range)# end`	
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range

Perform this task to configure the PPPoE session-count threshold for an individual PVC within an ATM PVC range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci
6. **pvc-in-range** [*pvc-name*] [*vpi* / *vci*]
7. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.

	Command or Action	Purpose
Step 4	**interface atm** *slot* / *subslot* / *port* [*.subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci **Example:** `Router(config-subif)# range range1 pvc 3/100 4/199`	Defines a range of ATM PVCs and enters ATM PVC Range configuration mode.
Step 6	**pvc-in-range** [*pvc-name*] [*vpi* / *vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Configures an individual PVC within a PVC range and enters ATM PVC-in-range configuration mode.
Step 7	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(cfg-if-atm-range-pvc)# pppoe max-sessions 10 threshold-sessions 5`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 8	**end** **Example:** `Router(cfg-if-atm-range-pvc)# end`	(Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Monitoring and Maintaining PPPoE Session Counts and SNMP Notifications

Perform the following task to monitor PPPoE sessions counts and SNMP notifications.

SUMMARY STEPS

1. **enable**
2. **debug snmp packets**
3. **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

4. **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
5. **show vpdn session**
6. **show pppoe session**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password when prompted.

Example:

```
Router> enable
```

Step 2 **debug snmp packets**

Use this command to display information about every SNMP packet sent or received by the router:

Example:

```
Router# debug snmp packets
SNMP: Packet received via UDP from 192.0.2.11 on GigabitEthernet1/0
SNMP: Get-next request, reqid 23584, errstat 0, erridx 0
 sysUpTime = NULL TYPE/VALUE
 system.1 = NULL TYPE/VALUE
 system.6 = NULL TYPE/VALUE
SNMP: Response, reqid 23584, errstat 0, erridx 0
 sysUpTime.0 = 2217027
 system.1.0 = Cisco Internetwork Operating System Software
 system.6.0 =
SNMP: Packet sent via UDP to 192.0.2.11
```

Step 3 **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.

Example:

```
Router# debug pppoe errors interface atm 1/0.10
PPPoE protocol errors debugging is on
Router#
00:44:30:PPPoE 0:Max session count(1) on mac(00b0.c2e9.c470) reached.
00:44:30:PPPoE 0:Over limit or Resource low. R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101
ATM1/0.10
```

Step 4 **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol messages about events that are part of normal session establishment or shutdown:

Example:

```
Router# debug pppoe events interface atm 1/0.10 vc 101

PPPoE protocol events debugging is on
Router#
```

```
00:41:55:PPPoE 0:I PADI  R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101 ATM1/0.10
00:41:55:PPPoE 0:O PADO, R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE 0:I PADR  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE :encap string prepared
00:41:55:[3]PPPoE 3:Access IE handle allocated
00:41:55:[3]PPPoE 3:pppoe SSS switch updated
00:41:55:[3]PPPoE 3:AAA unique ID allocated
00:41:55:[3]PPPoE 3:No AAA accounting method list
00:41:55:[3]PPPoE 3:Service request sent to SSS
00:41:55:[3]PPPoE 3:Created  R:0001.c9f0.0c1c L:00b0.c2e9.c470 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State REQ_NASPORT    Event MORE_KEYS
00:41:55:[3]PPPoE 3:O PADS  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State START_PPP    Event DYN_BIND
00:41:55:[3]PPPoE 3:data path set to PPP
00:41:57:[3]PPPoE 3:State LCP_NEGO    Event PPP_LOCAL
00:41:57:PPPoE 3/SB:Sent vtemplate request on base Vi2
00:41:57:[3]PPPoE 3:State CREATE_VA    Event VA_RESP
00:41:57:[3]PPPoE 3:Vi2.1 interface obtained
00:41:57:[3]PPPoE 3:State PTA_BIND    Event STAT_BIND
00:41:57:[3]PPPoE 3:data path set to Virtual Access
00:41:57:[3]PPPoE 3:Connected PTA
```

Step 5 show vpdn session

Use this command to display information about active Level 2 Forwarding (L2F) protocol tunnel and message identifiers on a VPDN:

Example:

```
Router# show vpdn session
%No active L2TP tunnels
%No active L2F tunnels
PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID        RemMAC          LocMAC       Intf    VASt    OIntf    VC
1       0010.7b01.2cd9  0090.ab13.bca8  Vi4     UP      AT6/0   0/10
```

Step 6 show pppoe session

Use this command to display information about the currently active PPPoE sessions:

Example:

```
Router# show pppoe session
     3 sessions in LOCALLY_TERMINATED (PTA) State
     3 sessions total

Uniq ID  PPPoE  RemMAC          Port            VT  VA         State
           SID  LocMAC                              VA-st      Type
      1      1  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.1      PTA
                001a.3045.0331  VC: 99/100          UP
      2      2  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.2      PTA
                001a.3045.0331  VC: 99/100          UP
      3      3  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.3      PTA
                001a.3045.0331  VC: 99/100          UP
Router#
```

Configuration Examples for Monitoring PPPoE Sessions with SNMP

Example: Configuring PPPoE Session-Count SNMP Traps

The following example shows how to enable the router to send PPPoE session-count SNMP notifications to the host at the address 192.10.2.10:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 192.10.2.10 version 2c public udp-port 1717
```

Example: Configuring PPPoE Session-Count Threshold for the Router

The following example shows a limit of 4000 PPPoE sessions configured for the router. The PPPoE session-count threshold is set at 3000 sessions, so when the number of PPPoE sessions on the router reaches 3000, an SNMP trap will be generated.

```
bba-group pppoe pppoe1
 sessions max limit 4000 threshold 3000
 virtual-template 1
pppoe limit max-sessions 4000 threshold-sessions 3000
```

Example: Configuring PPPoE Session-Count Threshold for a PVC

The following example shows a limit of five PPPoE sessions configured for the PVC. The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions on the PVC reaches three, an SNMP trap will be generated.

```
interface ATM 0/0/0
 ip address 10.0.0.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 5/120
  protocol ip 10.0.0.2 broadcast
  pppoe max-sessions 5 threshold-sessions 3
  protocol pppoe
```

Example: Configuring PPPoE Session-Count Threshold for a VC Class

The following example shows a limit of seven PPPoE sessions configured for a VC class called "main." The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions for the VC class reaches three, an SNMP trap will be generated.

```
vc-class atm main
  protocol pppoe group global
vc-class atm global
  protocol pppoe
  pppoe max-sessions 7 threshold-sessions 3
```

Example: Configuring PPPoE Session-Count Threshold for a PVC Range

The following example shows a limit of 20 PPPoE sessions configured for the PVC range. The PPPoE session-count threshold will also be 20 sessions because when the session-count threshold has not been explicitly configured, it defaults to the PPPoE session limit. An SNMP trap will be generated when the number of PPPoE sessions for the range reaches 20.

```
interface ATM 0/0/0.3 point-to-point
 range pvc 3/100 3/105
  pppoe max-sessions 20 threshold-sessions 15
  protocol pppoe
```

PPPoE Session-Count Threshold for an Individual PVC Within a PVC Range Example

The following example shows a limit of ten PPPoE sessions configured for pvc1. The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions for the PVC reaches three, an SNMP trap will be generated.

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 3/104
   pppoe max-sessions 10 threshold-sessions 3
```

Where to Go Next

- If you want to establish PPPoE session limits for sessions on a specific PVC or VLAN configured on an L2TP access concentrator, refer to the "Establishing PPPoE Session Limits per NAS Port" module.
- If you want to use service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup, refer to the "Offering PPPoE Clients a Selection of Services During Call Setup" module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to a LNS or tunnel switch, refer to the "Enabling PPPoE Relay Discovery and Service Selection Functionality" module.
- If you want to configure the transfer upstream of the PPPoX session speed value, refer to the "Configuring Upstream Connection Speed Transfer" module.
- If you want to identify a physical subscriber line for RADIUS communication with a RADIUS server, refer to the "Identifying the Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, refer to the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

The following sections provide references related to monitoring PPPoE sessions with SNMP.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Tasks for preparing for broadband access aggregation	Preparing for Broadband Access Aggregation
Configuring PPPoE sessions	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions
Establishing PPPoE session limits for sessions on a specific PVC or VLAN configured on an L2TP access concentrator	Establishing PPPoE Session Limits per NAS Port
Using service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup	Offering PPPoE Clients a Selection of Services During Call Setup
Enabling an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to a LNS or tunnel switch	Enabling PPPoE Relay Discovery and Service Selection Functionality
Configuring the transfer upstream of the PPPoX session speed value	Configuring Upstream Connection Speed Transfer
Identifying a physical subscriber line for RADIUS communication with a RADIUS server	Identifying the Physical Subscriber Line for RADIUS Access and Accounting
Configuring a Cisco Subscriber Service Switch	Configuring Cisco Subscriber Service Switch Policies

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
PPPoE Session Count MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

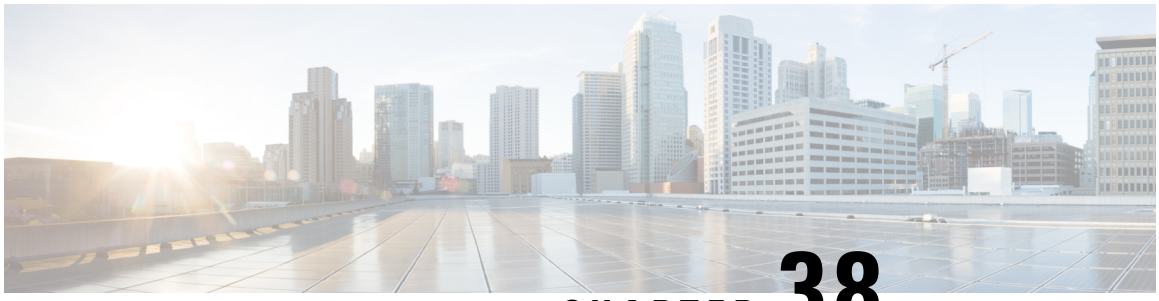
Feature Information for Monitoring PPPoE Sessions with SNMP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 45: Feature Information for Monitoring PPPoE Sessions with SNMP

Feature Name	Releases	Feature Configuration Information
PPPoE Session Count MIB, SNMP Traps for PPPoE Session Limits	Cisco IOS XE Release 2.5.0 Cisco IOS XE Release 2.6	This feature was introduced on Cisco ASR 1000 Series Aggregation Routers. This feature provides the ability to use SNMP to monitor in real time the number of PPP over Ethernet sessions configured on PVCs and on a router. You can also retrieve information from the MIB. The SNMP Traps for PPPoE Session Limits feature implements SNMP MIB support for the PPPoE session limits and generates notifications in case the limits are reached. The following commands were introduced or modified: **snmp-server enable traps pppoe**



CHAPTER 38

PPPoE on ATM

This feature module describes the PPP over Ethernet (PPPoE) on ATM feature. The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator.

Prerequisites for PPPoE on ATM

Before you can configure PPPoE on ATM, you need to specify a virtual template for the PPPoE sessions using the **virtual-template** command.

Restrictions for PPPoE on ATM

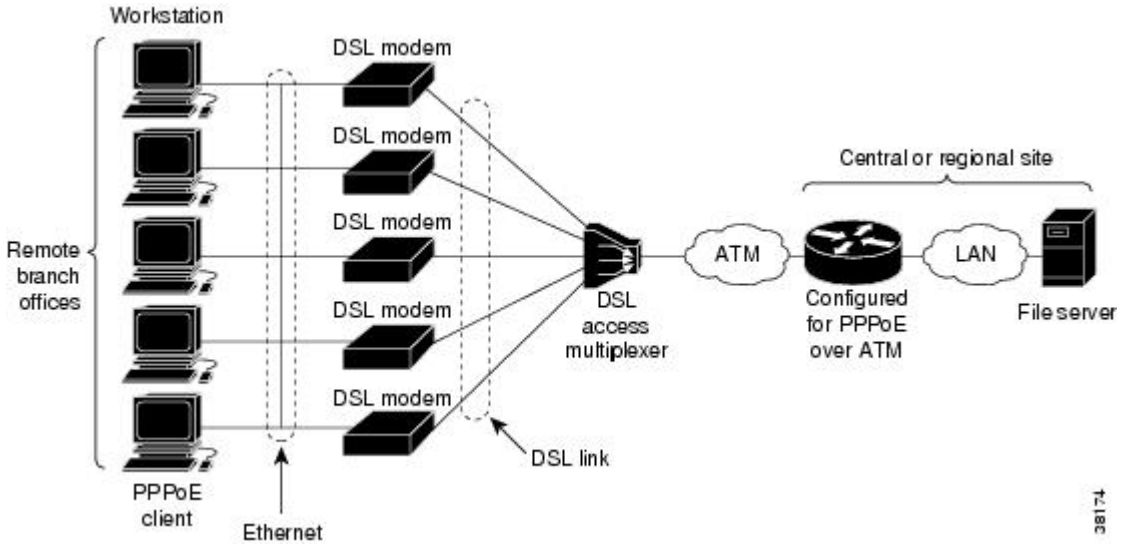
- PPPoE is not supported on Frame Relay.
- PPPoE over ATM AAl5Mux is not supported on ASR series 1000 routers. For more information, refer to the PPPoEoA over ATM AAL5Mux feature: http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_pppoeoa_aal5mux.html
- PPPoE is not supported on any other LAN interfaces such as FDDI and Token Ring.
- Fast switching is supported. PPPoE over RFC 1483 fibswitching is supported for IP. All other protocols are switched over process switching.
- Bridging is supported on the ATM permanent virtual connections (PVCs) running PPPoE.
- PPPoE is supported on ATM PVCs compliant with RFC 1483 only.
- Only dial-in mode is supported. Dial-out mode will not be supported.

Information About PPPoE on ATM

The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. With this model, each host utilizes its own PPPoE stack and the user is presented with a familiar user interface. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis. Before a point-to-point connection over Ethernet can be provided, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier. A unique session identifier is provided by the PPPoE Discovery Stage protocol.

The figure below shows a sample network topology using PPPoE on ATM.

Figure 31: PPPoE on ATM Sample Network Topology



PPPoE Stage Protocols

PPPoE has two distinct stage protocols. The stage protocols are listed and summarized in the table below.

Table 46: PPPoE Stage Protocols

Stage Protocols	Description
Discovery Stage protocol	Remains stateless until a PPPoE session is established. Once the PPPoE session is established, both the host and the access concentrator *must* allocate the resources for a PPP virtual access interface.
PPP Session Stage protocol	Once the PPPoE session is established, sends PPPoE data as in any other PPP encapsulation.

There are four steps to the Discovery Stage:

1. Host broadcasts a PPPoE Active Discovery Initiation (PADI) packet.
2. When the access concentrator receives a PADI that it can serve, it replies by sending a PPPoE Active Discovery Offer (PADO) packet to the host.

3. Because the PADI was broadcast, the host may receive more than one PADO packet. The host looks through the PADO packets it receives and chooses one. The choice can be based on the AC name or the services offered. The host then sends a single PPPoE Active Discovery Request (PADR) packet to the access concentrator that it has chosen.
4. When the access concentrator receives a PADR packet, it prepares to begin a PPP session. It generates a unique SESSION_ID for the PPPoE session and replies to the host with a PPPoE Active Discovery Session-confirmation (PADS) packet.

When a host wishes to initiate a PPPoE session, it must first perform discovery to identify the Ethernet MAC address of the peer and establish a PPPOE SESSION_ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client/server relationship. In the discovery process, a host (the client) discovers an access concentrator (the server). Based on the network topology, there may be more than one access concentrator that the host can communicate with. The Discovery Stage allows the host to discover all access concentrators and then select one. When discovery is completed, both the host and the selected access concentrator have the information they will use to build their point-to-point connection over Ethernet.

Benefits of PPPoE on ATM

The PPPoE on ATM feature provides service-provider digital subscriber line (DSL) support. As service providers begin DSL deployments, two of their most significant goals are to ease and facilitate consumer end adoption and to preserve as much of the dialup model as possible. PPPoE serves to advance both of these goals by leveraging ethernet scale curves and embedded base (such as ATM NICs) and by preserving the point-to-point session used by internet service providers (ISPs) in today's dialup model.

Using a PPPoE client (available from RouterWare), a PPP session can be initiated on an Ethernet connected client through a standard ADSL modem. The session is transported over the ATM DSL link via RFC 1483 Ethernet bridged frames and can terminate either in the LAN emulation client (LEC) central office or the ISP point of presence (POP). The termination device can be an aggregation box such as the Cisco 6400 or a router such as the Cisco 7200 series platforms.

As customers deploy asymmetric DSL (ADSL), they will encounter the need to enable users to access remote-access concentrators via simple bridges connecting Ethernet and ATM networks.

How to Configure PPPoE on ATM

Enabling PPP over ATM

After you configure the Cisco router or access server for Ethernet encapsulation, you must configure the physical interface with the PVC and apply a virtual template with PPP encapsulation to the PVC that it applies to. To configure the physical interface that will carry the PPPoE session and link it to the appropriate virtual template interface, use the following commands:

Note You can use the **virtual-template**, **sessions per-vc**, and **sessions per-mac** commands in any order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
6. **sessions per-mac limit** *per-mac-limit*
7. **exit**
8. **interface atm** *slot* / *subslot* / *port* [.*subinterface*][**point-to-point** | **multipoint**]
9. **ip address** *ip-address mask* [**secondary**]
10. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
11. **dbs enable** [**aggregated** | **maximum**]
12. Do one of the following:
    - **protocol pppoe group** {*group-name* | **global**}
    - or
    - **encapsulation aal5snap**
13. **create on-demand**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name*	**global**} **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 5	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]	Configures the PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets

	Command or Action	Purpose
	Example: `Router(config-bba-group)# sessions max limit 1`	the PPPoE session-count threshold at which an Simple Network Management Protocol (SNMP) trap will be generated. **Note** This command applies only to the global profile.
Step 6	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 4000`	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.
Step 7	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode and returns to global configuration mode.
Step 8	**interface atm** *slot / subslot / port* [*.subinterface*][**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 1/0.1 multipoint`	Specifies the ATM interface and enters subinterface configuration mode.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 192.0.10.2 255.255.255.0 secondary`	Sets a primary or secondary IP address for an interface.
Step 10	**range** [*range-name*] **pvc** *start-vpi / start-vci end-vpi / end-vci* **Example:** `Router(config-if)# range pvc 101/304 200/400`	Defines a range of ATM permanent virtual circuits (PVCs) and enters ATM range configuration mode.
Step 11	**dbs enable** [**aggregated** | **maximum**] **Example:** `Router(config-if-atm-range)# dbs enable`	Applies the Dynamic Subscriber Bandwidth Selection (DBS) QoS parameters.
Step 12	Do one of the following: • **protocol pppoe group** {*group-name* | **global**} • or • **encapsulation aal5snap** **Example:** `Router(config-if-atm-range-pvc)# protocol pppoe group two`	Enables PPPoE sessions to be established on a PVC within a range. or Configures PPPoE autosense. • If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

	Command or Action	Purpose
	Example: **Example:** **Example:** `Router(config-if-atm-range-pvc)# encapsulation aal5snap`	
Step 13	**create on-demand** **Example:** `Router(config-if-atm-range)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a range of PVCs to be created automatically on demand.
Step 14	**end** **Example:** `Router(config-if-atm-range)# end`	(Optional) Exits the ATM range configuration mode and returns to privileged EXEC mode.

Creating and Configuring a Virtual Template

Specifying an ATM Subinterface

After you create a virtual template for PPPoE on ATM, specify a multipoint or point-to-point subinterface per PVC connection. To specify an ATM multipoint subinterface, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* .*subinterface*] [**multipoint**| **point-to-point**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**interface atm** *slot* / *subslot* / *port* *.subinterface*] [**multipoint**| **point-to-point**] **Example:** `Router# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode. • A **multipoint** subinterface is recommended for interface conservation. A **point-to-point** subinterface will greatly restrict the total number of PPPoE sessions you can have.
Step 4	**end** **Example:** `Router(config-subif)# end`	(Optional) Exits the subinterface configuration mode and returns to privileged EXEC mode.

Creating an ATM PVC

Enabling PPPoE on an ATM PVC

To enable PPPoE on an ATM PVC, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* [*.subinterface*] [**multipoint** | **point-to-point**]
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **protocol pppoe**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 multipoint`	Configures the ATM interface and enters the subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 5/120`	Creates an ATM PVC and enters ATM VC configuration mode.
Step 5	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-vc)# pppoe max-sessions 5 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPPoE sessions to be established on ATM PVCs.
Step 7	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits the ATM VC configuration mode and returns to privileged EXEC mode.

Configuration Examples for PPPoE on ATM

PPPoE on ATM Example

The following example configures PPPoE on ATM to accept dial-in PPPoE sessions. The virtual access interface for the PPP session is cloned form virtual template interface 1. On subinterface ATM 2/0.1, ATM PVC with VPI 0 and VCI 60 is configured with Logical Link Control (LLC)/Subnetwork Access Protocol (SNAP) encapsulation and is configured to run PPPoE.

```
bba-group pppoe pppoe-group
 virtual-template 1
 sessions per-vc limit 1
 sessions per-mac limit 4000
interface atm 2/0.1 multipoint
 ip address 192.0.10.2 255.255.255.0 secondary
 range pvc 1/100 1/202
 pvc 0/60
  dbs enable
  encapsulation aal5snap
```

```
  protocol pppoe group two
  create on-demand
interface virtual-template 1
  ip addr 10.0.1.2 255.255.255.0
  mtu 1492
```

Where to Go Next

- If you want to enable PPP authentication on the virtual template using the **ppp authentication chap** command, refer to the "Configuring Virtual Template Interfaces" chapter in the *Cisco IOS Dial Solutions Configuration Guide* .
- If you want to configure an authentication, authorization, and accounting (AAA) server, refer to the "Configuring per-User Configuration" chapter in the *Cisco IOS Dial Solutions Configuration Guide* .

Additional References

The following sections provide references related to the PPPoE on ATM feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	
Broadband and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Enabling PPP authentication on the virtual template	Configuring Virtual Template Interfaces
Configuring an AAA server	Configuring per-User Configuration
Configuring Broadband and DSL	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1483	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*
RFC 2364	*PPP over AAL5*
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PPPoE on ATM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 47: Feature Information for PPPoE on ATM

Feature Name	Releases	Feature Information
PPPoE on ATM	Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature module describes the PPP over Ethernet (PPPoE) on ATM feature. The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. The following commands were introduced or modified: **bba-group, protocol (VPDN)**, **virtual-template**.

Glossary

AAL5 --ATM Adaptation Layer 5

ADSL --Asymmetric Digital Subscriber Line

ATM --Asynchronous Transfer Mode

CPCS --Common Part of Convergence Sublayer

CPI --Common Part Indicator

CRC --Cyclic Redundancy Check

DSLAM --Digital Subscriber Line Access Multiplexer

FCS --Frame Check Sequence

IETF --Internet Engineering Task Force

ID -Identifier

IP --Internet Protocol

L2TP --Layer two Tunneling Protocol

LAN --Local Area Network

LLC --Logical Link Control

MAC --Media Access Control

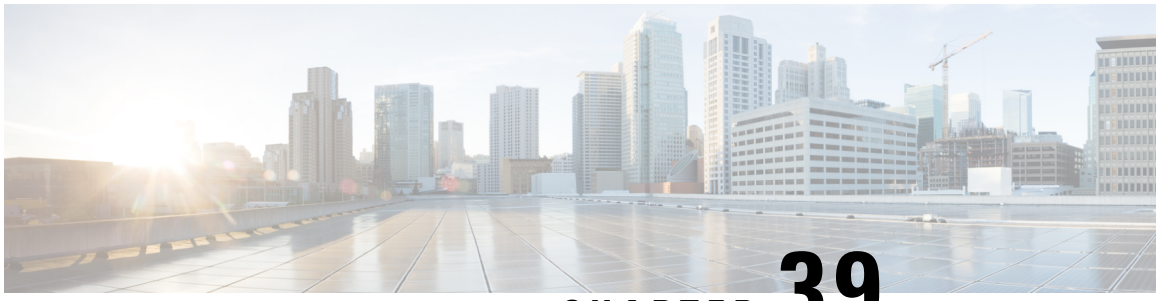
PDU --Protocol Data Unit

PPP --Point to Point Protocol

PPPoE --Point to Point Protocol over Ethernet

PVC --Permanent Virtual Connection

VPDN --Virtual Private Dialup Network



CHAPTER 39

PPPoE on Ethernet

The PPPoE on Ethernet feature adds support to Point-to-Point Protocol over Ethernet (PPPoE) by adding direct connection to actual Ethernet interfaces. PPPoE provides service-provider digital subscriber line (DSL) support. This Ethernet specification can be used by multiple hosts on a shared Ethernet interface to open PPP sessions to multiple destination with one or more bridging modems.

Prerequisites for PPPoE on Ethernet

Before you can configure the PPPoE on Ethernet feature, you need to configure a virtual private dialup network (VPDN) group using the **accept dialin** command, enable PPPoE, and specify a virtual template for PPPoE sessions.

Restrictions for PPPoE on Ethernet

- PPPoE is not supported on Frame Relay.
- PPPoE is not supported on any other LAN interfaces such as FDDI and Token Ring.
- Fast switching is supported. PPP over Ethernet over RFC 1483 fibswitching is supported for IP. All other protocols are switched over process switching.

Information About PPPoE on Ethernet

Benefits of Using PPPoE on Ethernet

Broadband Remote Access

For a bridged-Ethernet topology, the PPPoE on Ethernet feature allows access providers to maintain session abstraction associated with PPP networks.

PPPoE

PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator where each host utilizes its own PPP stack. It also gives users a familiar interface.

PPPoE provides service-provider DSL support. In service-provider DSL deployments, PPPoE leverages Ethernet scale curves and it uses an embedded base.

How to Enable and Configure PPPoE on Ethernet

Enabling PPPoE on Ethernet in a VPDN Group

To configure the physical interface that will carry the PPPoE session and link it to the appropriate virtual template interface, you need to complete the following steps.

SUMMARY STEPS

1. Router(config)# **vpdn enable**
2. Router(config-if)# **vpdn group** *name*
3. Router(config-if)# **accept dialin**
4. Router(config-if)# **protocol pppoe**
5. Router(config-if)# **virtual-template** *template-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **vpdn enable**	Enables virtual private dial-up networking.
Step 2	Router(config-if)# **vpdn group** *name*	Associates a VPDN group to a customer or VPDN profile.
Step 3	Router(config-if)# **accept dialin**	Creates an accept dial-in VPDN group.
Step 4	Router(config-if)# **protocol pppoe**	Specifies the VPDN group to be used to establish PPPoE sessions.
Step 5	Router(config-if)# **virtual-template** *template-number*	Specifies which virtual template will be used to clone virtual access interfaces.

Limiting PPPoE Sessions from a MAC Address

To set the limit of sessions to be sourced from a MAC address, use the following command in VPDN configuration mode:

Command	Purpose
`Router(config-if)# pppoe session-limit per-mac number`	Sets the limit of sessions to be sourced from a MAC address.

Creating and Configuring a Virtual Template

Other optional configuration commands can be added to the virtual template configuration. For example, you can enable the PPP authentication on the virtual template using the **ppp authentication chap** command. See the " Virtual Interface Template Service " chapter in the *Cisco IOS Dial S>olutions Configuration Guide* for more information about configuring the virtual template.

Although Cisco Express Forwarding switching is supported, flow, and optimum switching are not; these configurations are ignored on the PPPoE virtual access interface. Cisco Express Forwarding is enabled by default for IP. All other protocol traffic will be processed switched.

Note The PPP reliable link that uses Link Access Procedure, Balanced (LAPB) is not supported.

To create and configure a virtual template, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **interface virtual-template** *number*
2. Router(config-if)# **ip unnumbered ethernet** *number*
3. Router(config-if)# **mtu** *bytes*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface virtual-template** *number*	Creates a virtual template, and enters interface configuration mode.
Step 2	Router(config-if)# **ip unnumbered ethernet** *number*	Enables IP without assigning a specific IP address on the LAN.
Step 3	Router(config-if)# **mtu** *bytes*	Sets the maximum transmission unit (MTU) size for the interface.

Specifying an Ethernet Interface

After you create a virtual template for PPPoE on Ethernet, specify a multipoint or point-to-point interface. To specify an Ethernet multipoint interface, use the following commands in global configuration mode:

Command	Purpose
`Router# interface ethernet interface-number`	Specifies the Ethernet interface using the appropriate format of the **interface ethernet** command.

Enabling PPPoE on an Ethernet Interface

To enable PPPoE on Ethernet interfaces, use the following command in global configuration mode:

Command	Purpose
`Router# pppoe enable`	Specifies the VPDN group to be used for establishing PPPoE sessions.

Monitoring and Maintaining VPDN Groups

To monitor and maintain VPDN groups, use the following commands in EXEC mode:

Command	Purpose
`Router# show vpdn`	Displays information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN.
`Router# show vpdn session packet`	Displays PPPoE session statistics.
`Router# show vpdn session all`	Displays PPPoE session information for each session ID.
`Router# show vpdn tunnel`	Displays PPPoE session count for the tunnel.

Configuration Examples for PPPoE on Ethernet

PPPoE on Ethernet Example

The following are examples of the **vpdn enable** and **interface virtual-template** commands:

```
vpdn enable

 vpdn-group 1
```

```
accept dialin
protocol pppoe
virtual template 1
pppoe limit per-mac <number>

interface virtual-template 1
ip address 10.100.100.100 255.255.255.0
mtu 1492
```

For PPPoE virtual template interfaces, the **mtu** command must be configured because Ethernet has a maximum payload size of 1500 bytes, the PPPoE header is 6 bytes, and PPP Protocol ID is 2 bytes.

Note Dial-out mode will not be supported.

Enabling PPPoE on an Ethernet Interface Example

The following example enables PPPoE on an Ethernet interface:

```
interface ethernet1/0
 pppoe enable
```

Additional References

The following sections provide references related to the PPPoE on Ethernet feature.

Related Documents

Related Topic	Document Title
Configuring PPPoE on ATM	PPPoE over ATM
Configuring PPPoE on cable interfaces	• Point-to-Point Protocol over Ethernet Support on the Cisco CMTS • Configuring PPPoE Termination on a uBR7100 CMTS with L2TP Tunneling
Configuring PPPoE on IEEE 802.1Q encapsulation	PPPoE Over IEEE 802.1Q VLANs

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPPoE*
RFC 4813	Multiprotocol Encapsulation over ATM Adaptation Layer 5

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

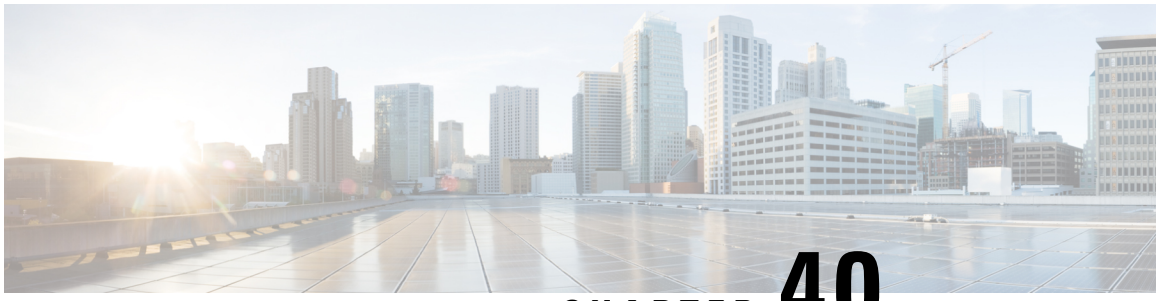
Feature Information for PPPoE on Ethernet

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 48: Feature Information for PPPoE on Ethernet

Feature Name	Releases	Feature Information
PPPoE on Ethernet	Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The PPPoE on Ethernet feature adds support to Point-to-Point Protocol over Ethernet (PPPoE) by adding direct connection to actual Ethernet interfaces. PPPoE provides service-provider digital subscriber line (DSL) support. This Ethernet specification can be used by multiple hosts on a shared Ethernet interface to open PPP sessions to multiple destination with one or more bridging modems.



CHAPTER 40

PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature provides two enhancements to PPP over Ethernet (PPPoE) over IEEE 802.1Q VLAN functionality:

- It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.
- It adds ATM permanent virtual circuit (PVC) support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation.

Restrictions for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

- PPPoE over IEEE 802.1Q VLAN support can be configured without using subinterfaces on the PPPoE server only.
- ATM PVC support for PPPoE over IEEE 802.1Q VLANs can be configured only on the PPPoE server.
- It is not possible to shut down traffic for individual VLANs that are configured on the main interface. Individual VLANs that are configured on subinterfaces can be shut down.

- A VLAN range can be configured on a main interface at the same time that VLANs outside the range are configured on subinterfaces of the same main interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time.
- PPPoE over VLAN Configuration on an interface is only supported for sessions that do not have Interface Descriptor Block (IDB). So this is not supported on ASR 1000 platforms.

Information About PPPoE over VLAN Configuration Limit Removal and ATM Support

To configure PPPoE over IEEE 802.1Q VLAN support on an interface rather than a subinterface, and to configure ATM support for PPPoE over IEEE 802.1Q VLANs, you should understand the following concepts:

PPPoE over VLAN Configuration Without Using Subinterfaces

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature removes the requirement for each PPPoE VLAN to be created on a subinterface. Allowing more than one PPPoE VLAN to be configured on a main interface increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

Individual VLANs or a range of VLANs can be configured on an interface. You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface.

PPPoE over VLAN Support on ATM PVCs

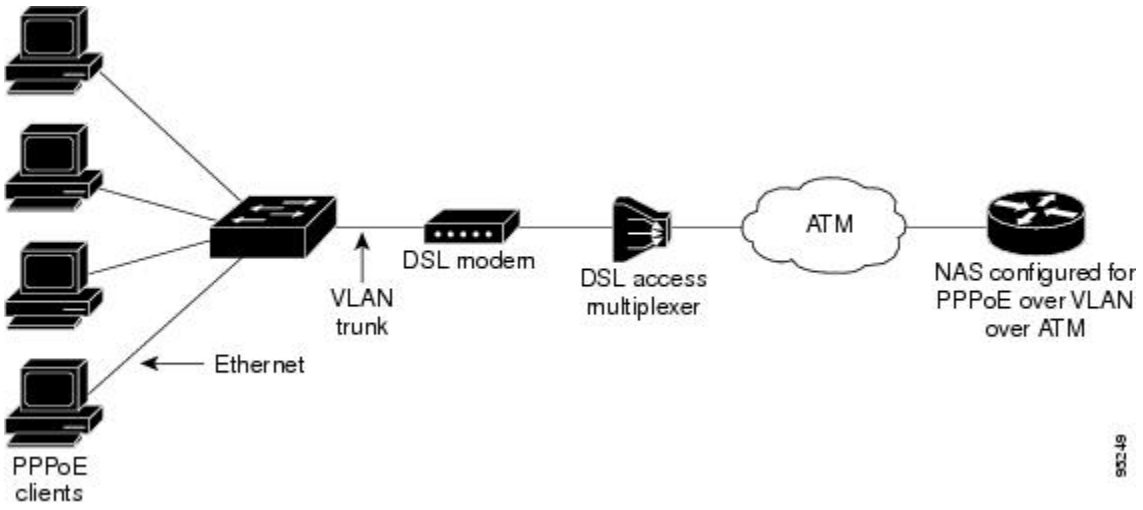
The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature enables ATM PVCs to process PPPoE over VLAN packets that use bridged RFC 1483 encapsulation. This capability allows PPPoE traffic from different IEEE 802.1Q VLANs to be multiplexed over the same ATM PVC.

The figure below shows a sample network topology that implements PPPoE over VLAN on ATM PVCs. In this topology, a service provider is using an Ethernet switch to provide Ethernet service to home users and a single PVC to provide the switch with WAN access. The home users use PPPoE to access services on the network access server (NAS). Each port on the switch is assigned a separate VLAN, and the VLANs are trunked over a Fast Ethernet or Gigabit Ethernet interface that is connected to a digital subscriber line (DSL) modem acting as a bridge.

The IEEE 802.1Q VLAN-encapsulated traffic coming in from the Ethernet switch trunk is encapsulated in RFC 1483 bridged encapsulation by the DSL modem and sent across the ATM WAN to the NAS. The NAS, which is configured to support PPPoE over VLANs over ATM PVCs, will extract the PPPoE packet from the PPPoE over IEEE 802.1Q VLAN over RFC 1483 bridged encapsulation and provide PPPoE services to the user.

In the downlink, the NAS sends packets in PPPoE over IEEE 802.1Q VLAN over RFC 1483 bridged encapsulation. The DSL modem strips off the RFC 1483 encapsulation and forwards the IEEE 802.1Q VLAN packets across the trunk to the switch. The switch then sends the Ethernet packets to the port associated with the IEEE 802.1 VLAN ID.

Figure 32: Sample Network Topology for PPPoE over IEEE 802.1Q VLANs over ATM



Benefits of PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature has the following benefits:

- Increases the number of VLANs that can be configured on a router to 4000 VLANs per interface by removing the requirement for each PPPoE VLAN to be configured on a subinterface.
- Provides support for PPPoE over VLANs over ATM interfaces using RFC 1483 bridged encapsulation

How to Configure PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

Configuring PPPoE over IEEE 802.1Q VLAN Support on an Ethernet Interface

Perform this task to configure PPPoE over IEEE 802.1Q VLAN support on an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **vlan-id dot1q** *vlan-id*
   -
   - **vlan-range dot1q** *start-vlan-id end-vlan-id*

5. **pppoe enable** [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/2`	Specifies the interface to be configured and enters interface configuration mode.

Step 4	Do one of the following:
	• **vlan-id dot1q** *vlan-id*
	•
	• **vlan-range dot1q** *start-vlan-id end-vlan-id*
	Example:
	`Router(config-if)# vlan-id dot1q 0`
	Example:
	Example:
	`Router(config-if)# vlan-range dot1q 0 60`
		Enables IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface.
		or
		Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface.

Step 5	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-if-vlan-range)# pppoe enable group pppoe1`	Enables PPPoE sessions over a specific VLAN or a range of VLANs.

Configuring an ATM PVC to Support PPPoE over IEEE 802.1Q VLAN Traffic

Perform this task to configure an ATM PVC to support RFC 1483 bridge encapsulated PPPoE over IEEE 802.1Q VLAN traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* **.** *subinterface-number* {**multipoint | point-to-point}**
4. **pvc** [*name*] *vpi* / *vci*
5. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **.** *subinterface-number* {**multipoint	point-to-point}** **Example:** `Router(config)# interface atm 2/0.1 multipoint`	Configures an ATM multipoint subinterface and enters subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 0/60`	Configures a PVC and enters ATM VC configuration mode.
Step 5	**protocol pppovlan dot1q** {*vlan-id*	*start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-if-atm-vc)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs on an ATM PVC.

Configuring a VC Class for PPPoE over IEEE 802.1Q VLAN Support

Perform this task to configure support for PPPoE over IEEE 802.1Q VLANs in a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*

4. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm class1`	Configures an ATM VC class and enters VC-class configuration mode.
Step 4	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-vc-class)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables support for PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs in a VC class. **Note** A VC class can be applied to an ATM interface, subinterface, PVC, or range of PVCs.

Monitoring and Maintaining PPPoE over IEEE 802.1Q VLAN

Perform this task to monitor and maintain PPPoE over VLAN connections.

SUMMARY STEPS

1. **enable**
2. **clear pppoe** {**interface** *type number* [**vc** {[*vpi/*]*vci* | *vc-name*}] [**vlan** *vlan-id*] | **rmac** *mac-address* [**sid** *session-id*] | **all**}
3. **debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number*[**vc** {[*vpi /*]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**clear pppoe** {**interface** *type number* [**vc** {[*vpi/*]*vci* | *vc-name*}] [**vlan** *vlan-id*] | **rmac** *mac-address* [**sid** *session-id*] | **all**} **Example:** `Router# clear pppoe interface fastethernet 0/2 vlan 1`	Clears PPPoE sessions.
Step 3	**debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number*[**vc** {[*vpi /*]*vci* | *vc-name*}] [**vlan** *vlan-id*]] **Example:** `Router# debug pppoe events interface atm 0/0 vc 1/16 vlan 10`	Displays debugging information for PPPoE sessions.

Configuration Examples for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

Configuring PPPoE over IEEE 802.1Q VLAN Support on an Ethernet Interface Example

The following example shows how to configure PPPoE over a range of IEEE 802.1Q VLANs on Fast Ethernet interface 0/0. The VLAN range is configured on the main interface and therefore each VLAN will not use up a separate subinterface.

```
bba-group pppoe PPPOE
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
  pppoe enable group PPPOE
  exit-vlan-config
```

Configuring PPPoE over IEEE 802.1Q VLAN Support on ATM PVCs Example

The following example shows how to configure an ATM PVC to support PPPoE over a range of IEEE 802.1Q VLANs:

```
bba-group pppoe PPPOEOA
```

```
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492
interface atm 4/0.10 multipoint
 pvc 10/100
  protocol pppovlan dot1q range 10 30 group PPPOEOA
```

Additional References

The following sections provide references related to the PPPoE Over VLAN Enhancements: Configuration Limit Removal and ATM Support feature.

Related Documents

Related Topic	Document Title
ATM PVC configuration	ATM chapter of the Cisco IOS Wide-Area Networking Configuration Guide
PPPoE and PPPoE over IEEE 802.1Q VLAN configuration	Broadband Access: PPP and Routed Bridge Encapsulation chapter of the Cisco IOS Wide-Area Networking Configuration Guide
VLAN range configuration (using subinterfaces)	VLAN Range feature module
ATM PVC and PPPoE configuration commands	Cisco IOS Wide-Area Networking Command Reference

Standards

Standard	Title
IEEE Standard 802.1Q, 1998	*Virtual Bridged Local Area Networks*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1483	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

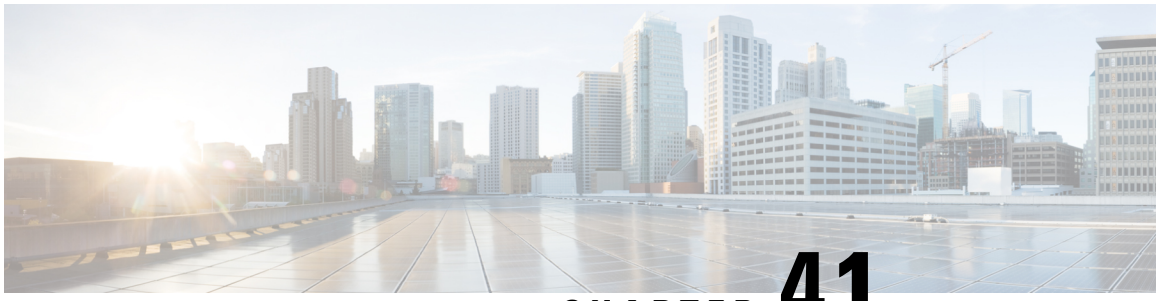
Feature Information for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 49: Feature Information for PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support

Feature Name	Releases	Feature Information
PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support	12.2 (31)SRC 12.3(2)T 12.2(33)SB Cisco IOS Release XE 3.9S	The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature provides two enhancements to PPP over Ethernet (PPPoE) over IEEE 802.1Q VLAN functionality: • It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router to 4000 VLANs per interface. • It adds ATM permanent virtual circuit (PVC) support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation. In Cisco IOS Release 12.2(31)SRC, this feature was introduced. In Cisco IOS Release 12.3(2)T, this feature was integrated into the T train. In Cisco IOS Release 12.2(33)SB, support was added for the Cisco IOS 10000 series routers. The following commands were introduced or modified: **clear pppoe** , **debug pppoe**, **pppoe enable**, **protocol pppovlan dot1q**, **vlan-id dot1q**, **vlan-range dot1q**.



CHAPTER 41

ADSL Support in IPv6

Asymmetric Digital Subscriber Line (ADSL) support in IPv6 provides the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on PPP links, per-user static routes, and ACLs.

Restrictions for ADSL Support in IPv6

ADSL and dial deployment are available for interfaces with PPP encapsulation enabled, including PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), PPP over async, and PPP over ISDN.

ADSL Support in IPv6

Address Assignment for IPv6

A Cisco router configured with IPv6 will advertise its IPv6 prefixes on one or more interfaces, allowing IPv6 clients to automatically configure their addresses. In IPv6, address assignment is performed at the network layer, in contrast to IPv4 where a number of functions are handled in the PPP layer. The only function handled in IPv6 control protocol is the negotiation of a unique interface identifier. Everything else, including Domain Name Server (DNS) server discovery, is done within the IPv6 protocol itself.

Contrary to IPv4 address assignment, an IPv6 user will be assigned a prefix, not a single address. Typically, the ISP assigns a 64- or 48-bit prefix.

In IPv6, ISPs assign long-lived prefixes to users, which has some impact on the routing system. In typical IPv4 environments, each network access server (NAS) has a pool of 24-bit addresses and users get addresses from this pool when dialing in. If a user dials another point of presence (POP) or is connected to another NAS at the same POP, a different IPv4 address is assigned.

Addresses for IPv6 are assigned using two methods:

Stateless Address Autoconfiguration

Assigning addresses using the stateless address autoconfiguration method can be used only to assign 64-bit prefixes. Each user is assigned a 64-bit prefix, which is advertised to the user in a router advertisement (RA). All addresses are automatically configured based on the assigned prefix.

A typical scenario is to assign a separate 64-bit prefix per user; however, users can also be assigned a prefix from a shared pool of addresses. Using the shared pool limits addresses to only one address per user.

This method works best for the cases where the customer provider edge (CPE) router is a single PC or is limited to only one subnet. If the user has multiple subnets, Layer 2 (L2) bridging, multilink subnets or proxy RA can be used. The prefix advertised in the RA can come from an authorization, authentication, and accounting (AAA) server, which also provides the prefix attribute, can be manually configured, or can be allocated from a prefix pool.

The Framed-Interface-Id AAA attribute influences the choice of interface identifier for peers and, in combination with the prefix, the complete IPv6 address can be determined.

How to Configure ADSL Support in IPv6

Configuring the NAS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **aaa new-model**
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authorization configuration default** {**radius** | **tacacs+**
7. **show ipv6 route** [*ipv6-address* | *ipv6-prefix* / *prefix-length* | *protocol* | *interface-type interface-number*
8. **virtual-profile virtual-template** *number*
9. **interface serial** *controller-number* **:** *timeslot*
10. **encapsulation** *encapsulation-type*
11. **exit**
12. **dialer-group** *group-number*
13. **ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]
14. **interface virtual-template** *number*
15. **ipv6 enable**
16. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
17. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-53a`	Specifies the hostname for the network server.
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA server.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default if-needed group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 6	**aaa authorization configuration default** {**radius** | **tacacs+** **Example:** `Router(config)# aaa authorization configuration default radius`	Downloads configuration information from the AAA server.
Step 7	**show ipv6 route** [*ipv6-address* | *ipv6-prefix* / *prefix-length* | *protocol* | *interface-type interface-number* **Example:** `Router(config)# show ipv6 route`	Shows the routes installed by the previous commands.
Step 8	**virtual-profile virtual-template** *number* **Example:** `Router(config)# virtual-profile virtual-template 1`	Enables virtual profiles by virtual interface template.

	Command or Action	Purpose
Step 9	**interface serial** *controller-number* **:** *timeslot* **Example:** `Router(config)# interface serial 0:15`	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signaling, or robbed-bit signaling). This command also puts the router into interface configuration mode.
Step 10	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 12	**dialer-group** *group-number* **Example:** `Router(config)# dialer-group 1`	Controls access by configuring an interface to belong to a specific dialing group.
Step 13	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 14	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 15	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 16	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 17	**radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*]	Specifies a RADIUS server host.

	Command or Action	Purpose
	[**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds* **Example:** `Router(config)# radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123`	

Configuring the Remote CE Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **interface bri** *number* **.** *subinterface-number* [**multipoint** | **point-to-point**]
5. **encapsulation** *encapsulation-type*
6. **ipv6 address autoconfig** [**default**
7. **isdn switch-type** *switch-type*
8. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
9. **ppp multilink** [**bap** | **required**]
10. **exit**
11. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
12. **ipv6 route** *ipv6-prefix* / *prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-36a`	Specifies the hostname for the network server.

	Command or Action	Purpose
Step 4	**interface bri** *number* **.** *subinterface-number* [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface bri 1.0`	Configures a BRI interface.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 6	**ipv6 address autoconfig** [**default** **Example:** `Router(config-if)# ipv6 address autoconfig`	Indicates that the IPv6 address will be generated automatically.
Step 7	**isdn switch-type** *switch-type* **Example:** `Router(config-if)# isdn switch-type basic-net3`	Specifies the central office switch type on the ISDN interface.
Step 8	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config-if)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 9	**ppp multilink** [**bap** | **required**] **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 12	**ipv6 route** *ipv6-prefix* / *prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*	Establishes static IPv6 routes. • Use one command for each route.

	Command or Action	Purpose
	Example: `Router(config)# ipv6 route 2001:DB8::1/128 BRI1/0`	

Configuration Examples for ADSL Support in IPv6

Example: NAS Configuration

This configuration for the ISP NAS shows the configuration that supports access from the remote CE router.

```
hostname cust1-53a
  aaa new-model
  aaa authentication ppp default if-needed group radius
  aaa authorization network default group radius
  virtual-profile virtual-template 1
  interface Serial0:15
   encapsulation ppp
   dialer-group 1
   ppp authentication chap
  !
  interface Virtual-Template1
   ipv6 enable
  !
  dialer-list 1 protocol ipv6 permit
  radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123
```

Example: Remote CE Router Configuration

This configuration for the remote customer edge router shows PPP encapsulation and IPv6 routes defined.

```
hostname cust-36a
  interface BRI1/0
   encapsulation ppp
   ipv6 enable
   isdn switch-type basic-net3
   ppp authentication chap optional
   ppp multilink
  !
  dialer-list 1 protocol ipv6 permit
  ipv6 route 2001:DB8::1/128 BRI1/0
  ipv6 route ::/0 2001:DB8::1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

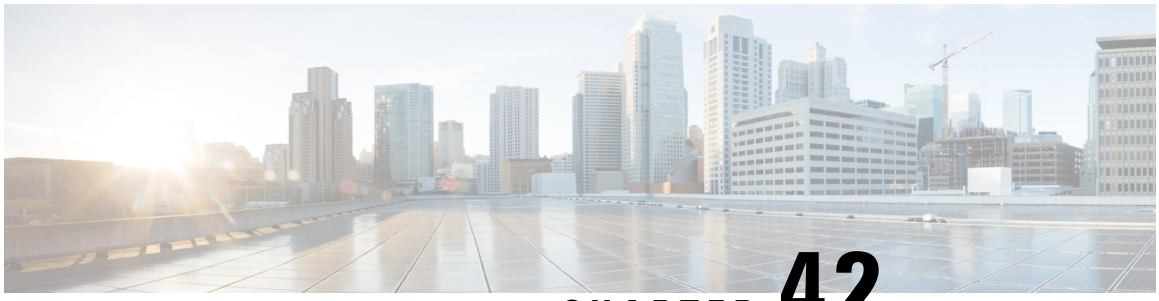
Feature Information for ADSL Support in IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 50: Feature Information for ADSL Support in IPv6

Feature Name	Releases	Feature Information
IPv6 ADSL and Dial Deployment Support	12.2(13)T	ADSL and dial deployment provide the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on PPP links, per-user static routes, and ACLs. The following commands were introduced or modified: **aaa authentication ppp**, **aaa authorization multicast default**, **aaa new-model**, **dialer-group**, **dialer-list**, **encapsulation**, **hostname**, **ipv6 address autoconfig**, **ipv6 route**, **isdn switch-type**, **ppp authentication**, **ppp multilink**, **radius-server host**, **show ipv6 route**, **virtual-profile virtual-template**.
IPv6 Access Services: PPPoA	12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoA.
IPv6 Access Services: PPPoE	12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoE.



CHAPTER 42

Broadband IPv6 Counter Support at LNS

Information About Broadband IPv6 Counter Support at LNS

Broadband IPv6 Counter Support at LNS

This feature provides support for broadband PPP IPv6 sessions at the layer 2 tunneling protocol (L2TP) network server (LNS). The sessions are forwarded by L2TP access concentrator (LAC) using layer 2 tunneling protocol L2TP over IPv6.

This feature is enabled automatically when the user configures LNS and enables IPv6.

How to Verify Broadband IPv6 Counter Support at LNS

Verifying Broadband IPv6 Counter Support at the LNS

This feature is enabled automatically when the user configures LNS and enables IPv6. To verify information about this feature, you can use any or all of the following optional commands as needed.

SUMMARY STEPS

1. **enable**
2. **show l2tp session** [**all** | **packets** [**ipv6**] | **sequence** | **state** | [**brief** | **circuit** | **interworking**] [**hostname**]] [**ip-addr** *ip-addr*[**vcid** *vcid*] | **tunnel** {**id** *local-tunnel-id local-session-id*| **remote-name** *remote-tunnel-name local-tunnel-name*}| **username** *username* | **vcid** *vcid*]
3. **show l2tp tunnel** [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name*| **remote-name** *remote-tunnel-name local-tunnel-name*]

4. **show l2tun session** [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets ipv6**] [*filter*] | **sequence** [*filter*] | **state** [*filter*]]
5. **show vpdn session** [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]]
6. **show vpdn tunnel** [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport**[*filter*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show l2tp session** [**all**	**packets** [**ipv6**]	**sequence**	**state**	[**brief**	**circuit**	**interworking**] [**hostname**]] [**ip-addr** *ip-addr*[**vcid** *vcid*]	**tunnel**{**id** *local-tunnel-id local-session-id*| **remote-name** *remote-tunnel-name local-tunnel-name*}| **username** *username*	**vcid** *vcid*] **Example:** `Router# show l2tp session packets ipv6`	Displays information about L2TP sessions.
Step 3	**show l2tp tunnel** [**all**	**packets** [**ipv6**]	**state**	**summary**	**transport**] [**id** *local-tunnel-id*	**local-name** *local-tunnel-name remote-tunnel-name*	**remote-name** *remote-tunnel-name local-tunnel-name*] **Example:** `Router# show l2tp tunnel packets ipv6`	Displays details about L2TP tunnels.
Step 4	**show l2tun session** [**l2tp**	**pptp**] [**all** [*filter*]	**brief** [*filter*] [**hostname**]	**circuit** [*filter*] [**hostname**]	**interworking** [*filter*] [**hostname**]	**packets ipv6**] [*filter*]	**sequence** [*filter*]	**state** [*filter*]] **Example:** `Router# show l2tun session packets ipv6`	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
Step 5	**show vpdn session** [**l2f**	**l2tp**	**pptp**] [**all**	**packets** [**ipv6**]	**sequence**	**state** [*filter*]] **Example:** `Router# show vpdn session packets ipv6`	Displays session information about active Layer 2 sessions for a virtual private dialup network (VPDN).
Step 6	**show vpdn tunnel** [**l2f**	**l2tp**	**pptp**] [**all** [*filter*]	**packets ipv6**] [*filter*]	**state** [*filter*]	**summary** [*filter*]	**transport**[*filter*]] **Example:**	Displays information about active Layer 2 tunnels for a VPDN.

	Command or Action	Purpose
	`Router# show vpdn tunnel packets ipv6`	

Configuration Examples for Broadband IPv6 Counter Support at LNS

Examples: Verifying Broadband IPv6 Counter Support at the LNS

Example: show l2tp session Command

The **show l2tp session** command used with the **packets and ipv6**keywords displays information about IPv6 packets and byte counts in an L2TP session.

```
Router# show l2tp session packets ipv6


L2TP Session Information Total tunnels 1 sessions 1


LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out

16791      53352      27723      30301740   30301742   20159754280 20523375360
```

Example: show l2tp tunnel Command

The **show l2tp tunnel** command used with the **packets** and **ipv6** keywords displays information about IPv6 packet statistics and byte counts in L2TP tunnels.

```
Router# show l2tp tunnel packets ipv6
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID   Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
27723      63060379   63060383   39400320490 40157045438
```

Example: show l2tun session Command

The **show l2tun session** command used with the **packets**and **ipv6**keywords displays information about IPv6 packet statistics and byte counts in an L2TUN session.

```
Router# show l2tun session packets ipv6
L2TP Session Information Total tunnels 1 sessions 1
LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
16791      53352      27723      31120707   31120708   21285014938 21658462236
```

Example: show vpdn session Command

The **show vpdn session** command used with the **l2tp**, **packets**, and **ipv6**keywords displays session information about IPv6 packet statistics and byte counts in an active layer 2 session for a VPDN.

```
Router# show vpdn session l2tp packets ipv6
L2TP Session Information Total tunnels 1 sessions 1
LocID       RemID       TunID       Pkts-In     Pkts-Out    Bytes-In    Bytes-Out
16791       53352       27723       35215536    35215538    22616342688 23038929320
```

Example: show vpdn tunnel Command

The **show vpdn tunnel**command used with the **l2tp**, **packets**, and **ipv6**keywords displays session information about IPv6 packet statistics and byte counts in an active layer 2 tunnel for a VPDN.

```
Device# show vpdn tunnel l2tp packets ipv6
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID    Pkts-In     Pkts-Out    Bytes-In    Bytes-Out
27723       61422447    61422451    37149801922 37886871686
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco_IOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

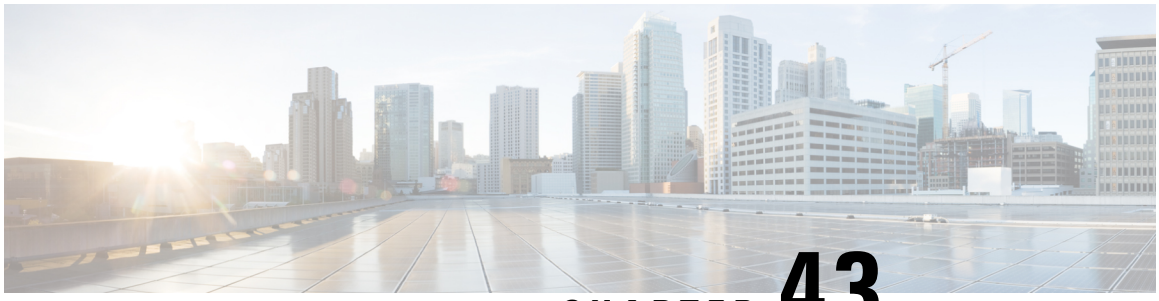
Feature Information for Broadband IPv6 Counter Support at LNS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 51: Feature Information for Broadband IPv6 Counter Support at LNS

Feature Name	Releases	Feature Information
Broadband IPv6 Counter Support at LNS	Cisco IOS XE Release 2.6	This feature provides support for broadband PPP IPv6 sessions at the L2TP LNS. The sessions are forwarded by LAC using layer 2 tunneling protocol L2TP over IPv4. The following commands were introduced or modified: **show l2tp session**, **show l2tp tunnel**, **show l2tun session**, **show vpdn session**, **show vpdn tunnel**.



CHAPTER 43

PPP IP Unique Address and Prefix Detection

The PPP IP Unique Address and Prefix Detection feature checks the uniqueness of IPv4 addresses and IPv6 prefixes on the broadband remote access server (BRAS). PPP disconnects the session if it detects a duplicate IPv4 address and IPv6 prefix.

Information About PPP IP Unique Address and Prefix Detection

- IPv6 checks if the prefix is unique when it is installed on an interface. If the prefix installation fails, PPP disconnects the session.
- PPP also checks if the IPv4 address is unique. PPP disconnects the session if a duplicate IPv4 address is detected.

How to Configure PPP IP Unique Address and Prefix Detection

Perform this task to configure the PPP IP Unique Address and Prefix Detection feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *interface-number*
4. **ppp ipcp address required**
5. **ppp ipcp address unique**
6. **ppp ipv6cp address unique**
7. **ppp timeout ncp** *seconds*
8. **exit**
9. **ppp ncp override local**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *interface-number* **Example:** `Router(config)# interface virtual-template 7`	Selects the Virtual Template interface and enters interface configuration mode.
Step 4	**ppp ipcp address required** **Example:** `Router(config-if)# ppp ipcp address required`	PPP disconnects the peer if no IP address is negotiated.
Step 5	**ppp ipcp address unique** **Example:** `Router(config-if)# ppp ipcp address unique`	PPP disconnects the peer if the IP address is already in use.
Step 6	**ppp ipv6cp address unique** **Example:** `Router(config-if)# ppp ipv6cp address unique`	PPP disconnects the peer if the IPv6 prefix is already in use.
Step 7	**ppp timeout ncp** *seconds* **Example:** `Router(config-if)# ppp timeout ncp 30`	PPP sets the maximum time in seconds to wait for the network layer to negotiate.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**ppp ncp override local** **Example:** `Router(config)# ppp ncp override local`	PPP overrides the local dual-stack configuration, checks the permitted Network Control Programs (NCP), and rejects user-initiated NCP negotiation.

	Command or Action	Purpose
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for PPP IP Unique Address and Prefix Detection

Example PPP Unique Address and Prefix Detection

To enable the PPP IP Unique Address nd Prefix Detection feature, use the following configuration.

```
Router# configure terminal
Router(config)# interface virtual-template 7

Router(config-if)# ppp ipcp address required

Router(config-if)# ppp ipcp address unique

Router(config-if)# ppp ipv6cp address unique

Router(config-if)# ppp timeout ncp 30
Router(config-if)# exit
Router(config)# ppp ncp override local
Router(config)# end
```

Additional References

Related Documents

Related Topic	Document Title
Broadband Access Aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

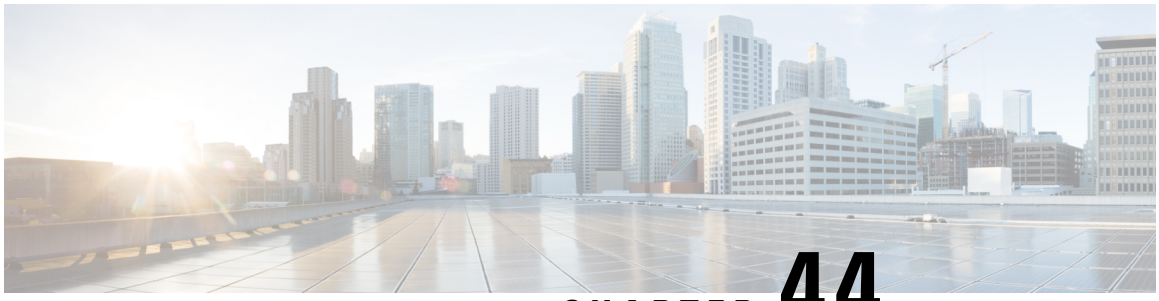
Feature Information for PPP IP Unique Address and Prefix Detection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 52: Feature Information for PPP IP Unique Address and Prefix Detection

Feature Name	Releases	Feature Information
PPP IP Unique Address and Prefix Detection	Cisco IOS XE Release 3.2S	The PPP IP Unique Address and Prefix Detection feature checks the uniqueness of IPv4 address and IPv6 prefix on the BRAS. PPP disconnects the session if it detects a duplicate IPv4 address and IPv6 prefix. The following commands were introduced: **ppp ipv6cp address unique**, **ppp ncp override local**.



CHAPTER 44

PPP IPv4 Address Conservation in Dual Stack Environments

The IPv4 Address Conservation in Dual Stack Environments feature enables service providers with a limited pool of IPv4 addresses to manage a large number of subscribers and conserve this address pool. A dual-stack environment is one in which service providers have both IPv4 addresses and IPv6 prefixes in their networks. A subscriber requests an IPv4 address, which it releases after a defined time interval. This same address can then be reassigned to any other subscriber, thereby allowing service providers to conserve the available IPv4 address space.

Prerequisites for PPP IPv4 Address Conservation in Dual Stack Environments

- You need to understand authentication, authorization, and accounting (AAA) and PPP before configuring IPv4 address conservation.
- A RADIUS server must be configured for centralized AAA.
- The customer premises equipment (CPE) must support a dual-stack environment and must have the intelligence to trigger the release of any IPv4 addresses not being used by applications at the CPE for a specified interval.
- The broadband remote access server (BRAS) must be able to send an IPv4 address request from a CPE device to the RADIUS server, a notification to the RADIUS server when an IPv4 address is allocated to the CPE device, and a notification to the RADIUS server when the CPE device releases the IPv4 address.
- The RADIUS server must be configured to assign only IPv6 prefixes during link control protocol (LCP) authentication, assign only IPv4 addresses when the BRAS sends an address allocation request, and

return released IPv4 addresses to the free pool of addresses in response to the BRAS IPv4 address-release notification.

Restrictions for PPP IPv4 Address Conservation in Dual Stack Environments

A local IP address pool must not be configured on the BRAS.

Information About PPP IPv4 Address Conservation in Dual Stack Environments

IPv4 Address Conservation in Dual Stack Environments

A subscriber in the service provider's network receives an IPv6 prefix from the RADIUS server in the initial authentication access-accept response. The broadband remote access server (BRAS) performs a uniqueness check to ensure that the IPv6 prefix has not been assigned to another subscriber. The BRAS then receives an Internet Protocol Control Protocol (IPCP) request for an IPv4 address from the subscriber. Next, the BRAS adds a number of attributes including the subscriber username and the Cisco vendor-specific attribute (VSA) for IPv4 address saving to the request, and sends this information to the RADIUS server. The VSA information tells the RADIUS server that this is a request for an existing session and the username identifies the subscriber making the request. The RADIUS server then sends an IPv4 address in the access-accept response. The BRAS checks that the IPv4 address that is to be assigned is not being used by any other subscriber. If a duplicate address is found, the session is torn down, otherwise the session is authorized. If the subscriber sends another request for an IPv4 address without terminating the earlier session, the BRAS does not send this request to the RADIUS server; instead, it uses the IPv4 address returned in the previous authorization exchange. When the subscriber terminates the session, the BRAS releases the IPv4 address and resets the authorization flag for this subscriber. This ensures that if the same subscriber requests an IPv4 address again, the request will be forwarded to the RADIUS server.

In addition, we recommend that you configure the following features on the BRAS. For a detailed description of the commands required to configure these features, see the Cisco IOS Broadband Access Aggregation and DSL Command Reference .

Note None of these features are mandatory for the IPv4 address conservation feature to work.

PPP IP Unique Address and Prefix Detection

The PPP IP Unique Address and Prefix Detection feature checks the uniqueness of IPv4 addresses and IPv6 prefixes on the broadband remote access server (BRAS). PPP disconnects the session if it detects a duplicate IPv4 address and IPv6 prefix.

PPP Local NCP Override

The PPP Local NCP Override feature configures the broadband remote access server (BRAS) to track the attributes received in the authorization from the RADIUS server, verifies the permitted Network Control Protocol (NCP), rejects the current NCP, and overrides the local dual-stack configuration.

AAA Delayed Accounting

The AAA Delayed Accounting feature delays the generation of accounting "start" records until the user IP address is established. When this feature is configured, the broadband remote access server (BRAS) sends an accounting "start" record to the RADIUS server when the appropriate network control protocol (NCP) is established.

How to Configure IPv4 Address Conservation in Dual Stack Environments

Configuring PPP IPv4 Address Conservation in Dual Stack Environments

Before you begin

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ppp ip address-save aaa-acct-vsa** *vsa-string*
4. **end**
5. **debug ppp ip address-save**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ppp ip address-save aaa-acct-vsa** *vsa-string* **Example:** `Router(config)# ppp ip address-save aaa-acct-vsa enable`	Enables IPv4 address conservation and defines the vendor-specific attribute value.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**debug ppp ip address-save** **Example:** `Router# debug ppp ip address-save`	Displays debugging information for the IPv4 address conservation feature.

Configuration Examples for PPP IPv4 Address Conservation in Dual Stack Environments

Example: PPP IPv4 Address Conservation in Dual Stack Environments

The following example shows how to enable the PPP IPv4 Address Conservation in Dual Stack Environments feature.

```
Router> enable
Router# configure terminal
Router(config)# ppp ip address-save aaa-acct-vsa enable
Router(config)# end
```

Additional References

Related Documents

Related Topic	Document Title
Broadband Access Aggregation and DSL commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

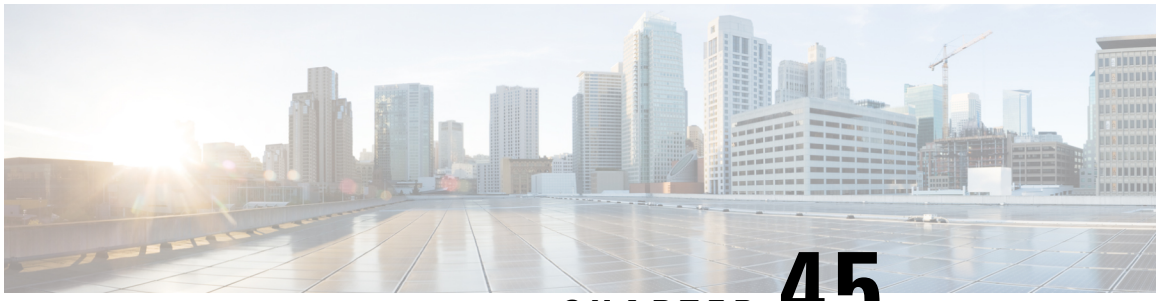
Feature Information for PPP IPv4 Address Conservation in Dual Stack Environments

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 53: Feature Information for PPP IPv4 Address Conservation In Dual Stack Environments

Feature Name	Releases	Feature Information
PPP IPv4 Address Conservation in Dual Stack Environments	Cisco IOS XE Release 3.5S	The IPv4 Address Conservation in Dual Stack Environments feature enables service providers with a limited pool of IPv4 addresses to manage a large number of subscribers and conserve this address pool. A subscriber is allocated an IPv4 address, which it releases after a defined time interval. This same address can then be reassigned to another subscriber that requests an IPv4 address. The following commands were introduced: **debug ip address-save**, **ppp ip address-save aaa-acct-vsa**.



CHAPTER 45

Broadband High Availability Stateful Switchover

The Cisco IOS XE Broadband High Availability Stateful Switchover feature provides the capability for dual Route Processor systems to support stateful switchover of Point-to-Point Protocol over X (PPPoX, where X designates a family of encapsulating communications protocols such as PPP over Ethernet [PPPoE], PPP over ATM [PPPoA], PPPoEoA, PPPoEoVLAN implementing PPP) sessions, thus allowing applications and features to maintain a stateful state while system control and routing protocol execution is transferred between an active and a standby processor.

Prerequisites for Broadband High Availability Stateful Switchover

The stateful switchover (SSO) and nonstop forwarding (NSF) features must be enabled. For more information about SSO, see the "Stateful Switchover" module. For more information about NSF, see the "Configuring Nonstop Forwarding" module.

Restrictions for Broadband High Availability Stateful Switchover

SSO is supported only on High Availability (HA) network devices.

Information About Broadband High Availability Stateful Switchover

Feature Design of Broadband High Availability Stateful Switchover

Prior to the implementation of the Broadband High Availability Stateful Switchover feature, unplanned control plane and dataplane failures resulted in service outages and network downtime for PPPoX sessions. Cisco HA features, including SSO, enable network protection by providing fast recovery from such failures. The Broadband High Availability Stateful Switchover feature eliminates a source of outages by providing for stateful switchover to a standby processor while continuing to forward traffic. SSO protects from hardware or software faults on an active Route Processor (RP) by synchronizing protocol and state information for supported features with a standby RP, ensuring no interruption of sessions or connections if a switchover occurs.

The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor, designating the other RP as the standby processor, and then synchronizing critical state information between them. Following an initial (bulk) synchronization between the two processors, SSO dynamically maintains RP state information between them. A switchover from the active to the standby processor occurs when the active RP fails, when it is removed from the networking device, or when it is manually taken down for maintenance. The standby RP then takes control and becomes the active RP, preserving the sessions and connections for the supported features. At this time, packet forwarding continues while route convergence is completed on the newly active RP. A critical component of SSO and Cisco HA technology is the cluster control manager (CCM) that manages session re-creation on the standby processor. The Broadband High Availability Stateful Switchover feature allows you to configure subscriber redundancy policies that tune the synchronization process. For more information, see the Configuring Subscriber Redundancy Policy for Broadband HA Stateful Switchover, on page 498.

The Broadband High Availability Stateful Switchover feature works with the Cisco NSF and SSO HA features, to maintain PPPoX sessions. NSF forwards network traffic and application state information so that user session information is maintained after a switchover.

For information about High Availability and stateful switchover, see the "High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide .

Supported Broadband Aggregation Protocols

The Broadband High Availability Stateful Switchover feature set supports the broadband aggregation protocols described in the following sections:

SSO PPPoA

The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over ATM (PPPoA) sessions during Route Processor switchover.

SSO L2TP

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic stateful switchover/In Service Software Upgrade (SSO/ISSU) mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access

Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

SSO PPPoE

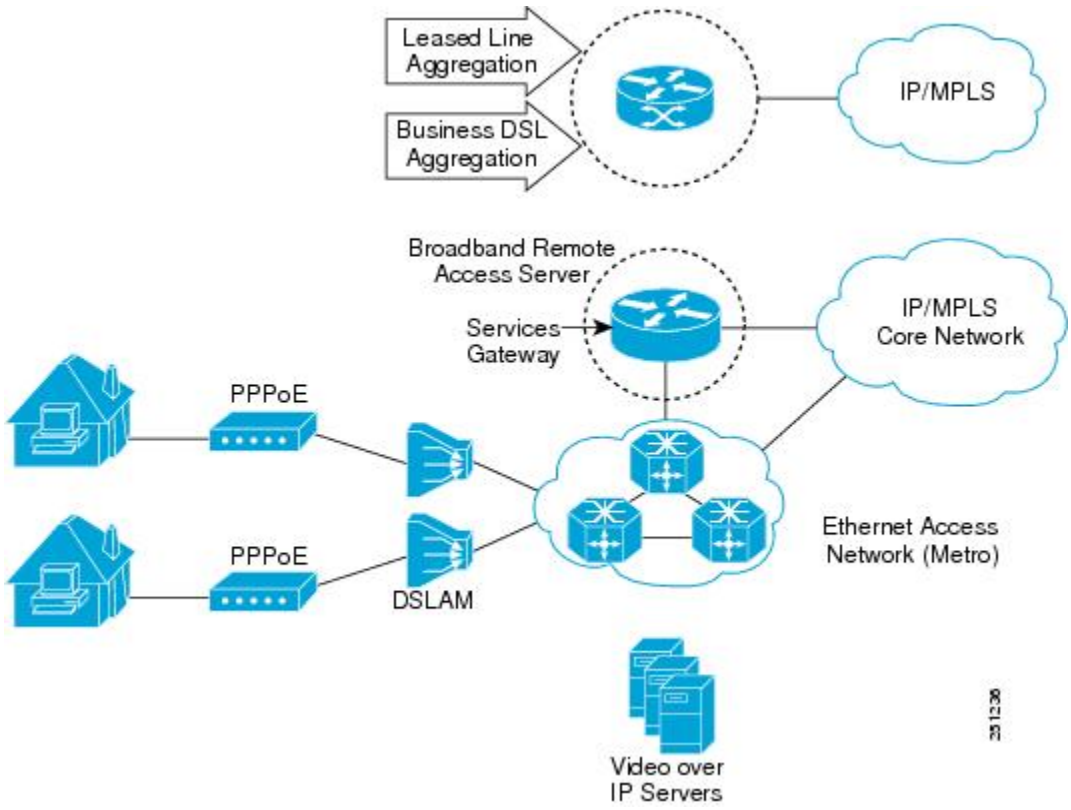
The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoEoVLAN, and PPPoEoQinQ.

SSO RA-MLPS VPN

The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPPoX terminated into remote access (RA)-Multiprotocol Label Switching (MPLS) VPN or PPPoX into MPLS VPN sessions during processor switchover.

The figure below shows a typical broadband aggregation HA deployment with SSO functionality.

Figure 33: Broadband Aggregation High Availability Deployment



Benefits of Broadband High Availability Stateful Switchover

- Reduces operating costs associated with outages.
- Delivers higher service levels to subscribers.
- Improves network availability.

- Promotes continuous connectivity, lower packet loss, and consistent path flow through nodes providing specific network services.
- Mitigates service disruptions, reduces downtime costs, and increases operational efficiency.

How to Configure Broadband High Availability Stateful Switchover

Configuring Subscriber Redundancy Policy for Broadband HA Stateful Switchover

Perform this task to configure subscriber redundancy policy for HA SSO capability for broadband subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy { bulk limit { cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | time** *seconds* **} | dynamic limit cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | delay** *seconds* **| rate** *sessions seconds* **}**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber redundancy { bulk limit { cpu** *percent* **delay** *seconds* **[allow** *sessions* **]	time** *seconds* **}	dynamic limit cpu** *percent* **delay** *seconds* **[allow** *sessions* **]	delay** *seconds* **| rate** *sessions seconds* **}** **Example:** `Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`	(Optional) Configures subscriber redundancy policy. • **bulk** --Configures bulk synchronization redundancy policy. • **limit** --Specifies the limit for the synchronization. • **cpu** *percent* --Specifies a CPU busy threshold value as a percentage. Range is from 0 to 100; default is 90.

	Command or Action	Purpose

		• **delay** *seconds* --Specifies the minimum amount of time, in seconds, that a session must be ready before bulk or dynamic synchronization occurs. Range is from 1 to 33550.
		• **allow** *sessions* --(Optional) Specifies the minimum number of sessions to synchronize once the CPU busy threshold is exceeded and the specified delay is met. Range is from 1 to 2147483637; default is 25.
		• **dynamic** --Configures a dynamic synchronization redundancy policy.
		• **rate** *sessions seconds* --Specifies the number of sessions per time period for bulk and dynamic synchronization.
		  • *sessions*--Range is from 1 to 32000; default is 250.
		  • *seconds*--Range in seconds is from 1 to 33550; default is 1.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA Stateful Switchover

To view the configuration, use the **show running-config** command. Sample output is available at Configuration Examples for Broadband High Availability Stateful Switchover, on page 505.

SUMMARY STEPS

1. **show ccm clients**
2. show ccm sessions
3. show ppp subscriber statistics
4. **show pppatm statistics**
5. **show pppoe statistics**
6. **show vpdn redundancy**
7. **show vpdn history failure**
8. **show pppatm redundancy**
9. **show pppoe redundancy**
10. **debug pppatm redundancy**
11. **debug pppoe redundancy**

DETAILED STEPS

Step 1 **show ccm clients**

Example:

```
This command is useful for troubleshooting the CCM synchronization component. This command displays
 information about the CCM, which is the HA component that manages the capability to synchronize
session launch on the standby processor of a redundant processor HA system.
```

Active Route Processor

Example:

```
Router# show ccm clients
CCM bundles sent since peer up:
Sent Queued for flow control
Sync Session 16000 0
Update Session 0 0
Active Bulk Sync End 1 0
Session Down 0 0
ISSU client msgs 346 0
Dynamic Session Sync 0 0
Unknown msgs 0 0
Client events sent since peer up:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

Standby Route Processor

Example:

```
Router# show ccm clients

CCM bundles rcvd since last boot:
Sync Session 16000
Update Session 0
Active Bulk Sync End 1
Session Down 0
ISSU client msgs 173
Dynamic Session Sync 0
Unknown msgs 0
Client events extracted since last boot:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

Step 2 show ccm sessions

This command is useful for troubleshooting the CCM synchronization component. This command shows information about sessions managed by CCM.

Active Route Processor

Example:

```
Router# show ccm sessions
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFE
Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 9279
Number of sessions in state Ready: 0 0 6721
Number of sessions in state Dyn Sync: 16000 16000 0
Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 64 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 475 - -
```

Standby Route Processor

Example:

```
Router# show ccm sessions

Global CCM state: CCM HA Standby - Collecting
Global ISSU state: Compatible, Clients Cap 0x9EFFE
Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 8384
Number of sessions in state Ready: 16000 0 7616
Number of sessions in state Dyn Sync: 0 0 0
Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 0 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 0 - -
```

Step 3 show ppp subscriber statistics

This command is useful for reviewing PPPoX session statistics. Use the **show ppp subscriber statistics** command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the **clear ppp subscriber statistics** command was last issued.

The following is sample output from the **show ppp subscriber statistics** command:

Example:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
```

```
LocalTerm                     7             7
LocalTermVP                   0             0
MoreKeys                      7             7
Forwarding                    0             0
Forwarded                     0             0
SSSDisc                       0             0
SSMDisc                       0             0
PPPDisc                       0             0
PPPBindResp                   7             7
PPPReneg                      3             3
RestartTimeout                5             5
PPP Subscriber Statistics     TOTAL         SINCE CLEARED
IDB CSTATE UP                 4             4
IDB CSTATE DOWN               8             8
APS UP                        0             0
APS UP IGNORE                 0             0
APS DOWN                      0             0
READY FOR SYNC                8             8
```

Step 4 **show pppatm statistics**

This command is useful for obtaining statistics for PPPoA sessions. Use the **show pppatm statistics** command to display a total count of PPPoA events since the **clear pppatm statistics**command was last issued.

The following example displays PPPoA statistics:

Example:

```
Router# show pppatm statistics
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

Step 5 **show pppoe statistics**

This command is useful for reviewing PPPoX session statistics. Use the **show pppoe statistics** command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the **clear pppoe statistics** command was last issued.

The following is sample output from the **show pppoe statistics** command:

Example:

```
Router# show pppoe statistics
PPPoE Events                  TOTAL         SINCE CLEARED
----------------------------- ------------- -------------
INVALID                       0             0
PRE-SERVICE FOUND             0             0
PRE-SERVICE NONE              0             0
SSS CONNECT LOCAL             0             0
SSS FORWARDING                0             0
SSS FORWARDED                 0             0
```

```
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM DISCONNECT                 0             0
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        0             0
PPPoE Handles Freed            0             0
Dynamic Bind Request           0             0
Static Bind Request            0             0
```

Step 6 **show vpdn redundancy**

Use this command to verify the failure of any L2TP tunnels.

Example:

```
Router# show vpdn redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
Checkpoint Messaging on: FALSE
Standby RP is up: TRUE
Recv'd Message Count: 0
L2TP Tunnels: 2/2/2/0 (total/HA-enabled/HA-est/resync)
L2TP Sessions: 10/10/10 (total/HA-enabled/HA-est)
L2TP Resynced Tunnels: 0/0 (success/fail)
```

Step 7 **show vpdn history failure**

Use this command to verify the failure of any VPDN groups.

Example:

```
Router# show vpdn history failure

% VPDN user failure table is empty
```

Step 8 **show pppatm redundancy**

Use the **show pppatm redundancy** command to display the PPPoA HA sessions summary. The following is sample output from the **show pppatm redundancy** command from a Cisco 10000 series router standby processor:

Example:

```
Router-stby# show pppatm redundancy
0 : Session recreate requests from CCM
0 : Session up events invoked
0 : Sessions reaching PTA
0 : Sessions closed by CCM
0 : Session down events invoked
0 : Queued sessions waiting for base hwidb creation
0 : Sessions queued for VC up notification so far
```

```
0 : Sessions queued for VC encap change notification so far
0 : VC activation notifications received from ATM
0 : VC encap change notifications received from ATM
0 : Total queued sessions waiting for VC notification(Encap change+VC Activation)
```

Step 9 **show pppoe redundancy**

This command is useful for reviewing PPPoX session statistics. Use the **show pppoe redundancy** command to display statistics and events for PPPoE sessions. This command gives a cumulative count of PPPoE events and statistics, and an incremental count since the **clear pppoe redundancy** command was last issued.

The following is sample output from the **show pppoe redundancy** command from a Cisco 10000 series router standby processor:

Example:

```
Router-stby# show pppoe redundancy
12 Event Queues
size max kicks starts false suspends ticks(ms)
9 PPPoE CCM EV 0 1 2 3 1 0 20
Event Names
Events Queued MaxQueued Suspends usec/evt max/evt
1* 9 Recreate UP 2 0 1 0 1500 3000
2* 9 Recreate DOWN 0 0 0 0 0 0
3* 9 VC Wait UP 0 0 0 0 0 0
4* 9 VC Wait Encap 0 0 0 0 0 0
Sessions waiting for Base Vaccess: 0
Sessions waiting for ATM VC UP: 0
Sessions waiting for Auto VC Encap 0
```

Step 10 **debug pppatm redundancy**

Use the **debug pppatm redundancy** command to display CCM events and messages for PPPoA sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes. The following is sample output from the **debug pppatm redundancy** command from a Cisco 10000 series router active processor:

Example:

```
Router# debug pppatm redundancy
PPP over ATM redundancy debugging is on
```

Step 11 **debug pppoe redundancy**

Use the **debug pppoe redundancy** command to display CCM events and messages for PPPoE sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppoe redundancy
Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
```

```
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

Configuration Examples for Broadband High Availability Stateful Switchover

Example Configuring Broadband High Availability Stateful Switchover

The following example shows how to configure the Broadband High Availability Stateful Switchover feature:

```
Router# configure terminal
Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30
Router(config)# exit
```

The following is a sample configuration of PPPoX terminated into an RA-MPLS network with SSO. Commands that appear in the configuration task tables for this feature but that do not appear in the running configuration output are configured for their default settings.

```
Router# show running-config
hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

The following lines show the subscriber redundancy policy configuration:

```
subscriber redundancy dynamic limit cpu 90 delay 10
```

```
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
  virtual-template 2
!
bba-group pppoe grp3
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 10.1.1.1 255.255.255.255
!
interface Loopback100
  ip address 192.168.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
encapsulation dot1Q 2
pppoe enable group grp2
!
!
```

```
interface GigabitEthernet1/0/1
no ip address
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
encapsulation dot1Q 2
pppoe enable group grp5
!
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
!
interface GigabitEthernet7/0/3
no ip address
!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
```

```
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
```

```
  network 224.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 224.0.0.3 remote-as 1
  neighbor 224.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 224.0.0.3 activate
  neighbor 224.0.0.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.13.1.1 10.13.16.160
ip local pool pool4 10.14.1.1 10.14.16.160
ip local pool pool5 10.15.1.1 10.15.16.160
ip local pool pool6 10.16.1.1 10.16.16.160
ip local pool pool7 10.17.1.1 10.17.16.160
ip local pool pool8 10.18.1.1 10.18.16.160
ip classless !
!
no ip http server
!
!
arp 10.20.1.1 0020.0001.0001 ARPA
arp vrf vrf1 10.20.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Broadband Access Aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
High Availability	"High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide

Related Topic	Document Title
Performing an ISSU	The following chapters in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide : • "Cisco IOS XE Software Package Compatibility for ISSU" • "In Service Software Upgrade (ISSU)"
Broadband ISSU	"Broadband High Availability In Service Software Upgrade" module
Stateful switchover	"Stateful Switchover" module
Configuring nonstop forwarding	"Configuring Nonstop Forwarding" module
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

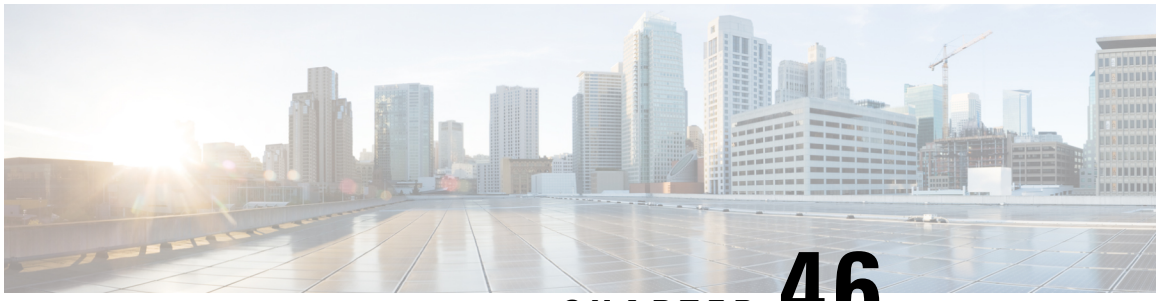
Feature Information for Broadband High Availability Stateful Switchover

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 54: Feature Information for the Broadband High Availability Stateful Switchover Feature

Feature Name	Releases	Feature Information
SSO--PPPoA	Cisco IOS XE Release 3.3S	In Cisco IOS XE Release 3.3S, this feature was implemented on ASR 1000 Series Routers. The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over ATM (PPPoA) sessions during RP switchover. The following commands were introduced or modified: **subscriber redundancy**, **debug pppatm redundancy**, **debug pppoe redundancy**, **show pppoe redundancy**, **show pppatm statistics**.
SSO--PPPoE	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.1, this feature was implemented on ASR 1000 Series Routers. This feature uses the SSO--PPPoE feature to provide the capability for dual Route Processor systems to support stateful switchover of PPPoX sessions and allow applications and features to maintain state while system control and routing protocol execution is transferred between an active and a standby processor. The following commands were introduced or modified: **clear ppp subscriber statistics**, **clear pppoe statistics**, **debug pppoe redundancy, show ccm clients, show ccm sessions, show ppp subscriber statistics, show pppoe statistic, subscriber redundancy**.



CHAPTER 46

Broadband High Availability In-Service Software Upgrade

The Broadband High Availability (HA) In-Service Software Upgrade (ISSU) feature ensures continuous operations of broadband access protocols during software upgrades, downgrades, and service enhancements.

Prerequisites for Broadband High Availability In-Service Software Upgrade

The ISSU and nonstop forwarding (NSF) features must be enabled. For more information about In-Service Software Upgrade, see the "Performing an In Service Software Upgrade" module. For more information about NSF, see the "Configuring Nonstop Forwarding" module.

Restrictions for Broadband High Availability In-Service Software Upgrade

- You can perform an ISSU across a major Cisco IOS XE release.
- You can perform an ISSU from a Cisco IOS XE release that supports ISSU capability.

Information About Broadband High Availability In-Service Software Upgrade

Feature Design of Broadband High Availability In-Service Software Upgrade

Prior to the implementation of the Broadband High Availability In-Service Software Upgrade feature, software upgrades typically required planned outages that took the router or network out of service. The Broadband High Availability In-Service Software Upgrade feature enables the service provider to maximize network availability and eliminate planned outages by allowing the Cisco IOS XE release to be upgraded without taking the router or network out of service. ISSU is a procedure, based on Cisco high availability (HA) architecture, whereby the Cisco IOS XE infrastructure accomplishes an upgrade while packet forwarding continues and broadband sessions are maintained. Cisco HA architecture is based on redundant Route Processors and the NSF and SSO features, such that ports stay active and calls do not drop, eliminating network disruption during upgrades.

The ISSU feature allows deployment of new features, hardware, services, and maintenance fixes in a procedure that is seamless to end users. A critical component of ISSU and Cisco HA technology is the cluster control manager (CCM) that manages session recreation and synchronization on the standby processor. The Broadband High Availability In-Service Software Upgrade feature allows the configuration of subscriber redundancy policies that tune the synchronization process. For more information see the Configuring Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade, on page 516 .

The Broadband High Availability In-Service Software Upgrade feature handles upgrades and downgrades, and supports the following:

- Upgrades from one software feature release to another, as long as both versions support the ISSU feature, for example, from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3.
- Upgrades from one software maintenance release to another, for example from Cisco IOS XE Release 2.2.1 to Cisco IOS XE Release 2.2.2.

The Broadband High Availability In-Service Software Upgrade feature works with other Cisco IOS XE HA features, NSF and SSO, to maintain broadband sessions.

Performing an ISSU

For detailed information about HA and about performing an ISSU, see the following chapters in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide :

- "High Availability Overview"
- "Cisco IOS XE Software Package Compatibility for ISSU"
- "In Service Software Upgrade (ISSU)"

Supported Broadband Aggregation Protocols

The Broadband High Availability In-Service Software Upgrade feature supports the following broadband aggregation protocols described in the following sections:

ISSU PPPoA

The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPP over ATM (PPPoA) sessions during supported software upgrades, downgrades, and enhancements.

ISSU L2TP

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic SSO/ISSU mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

ISSU PPPoE

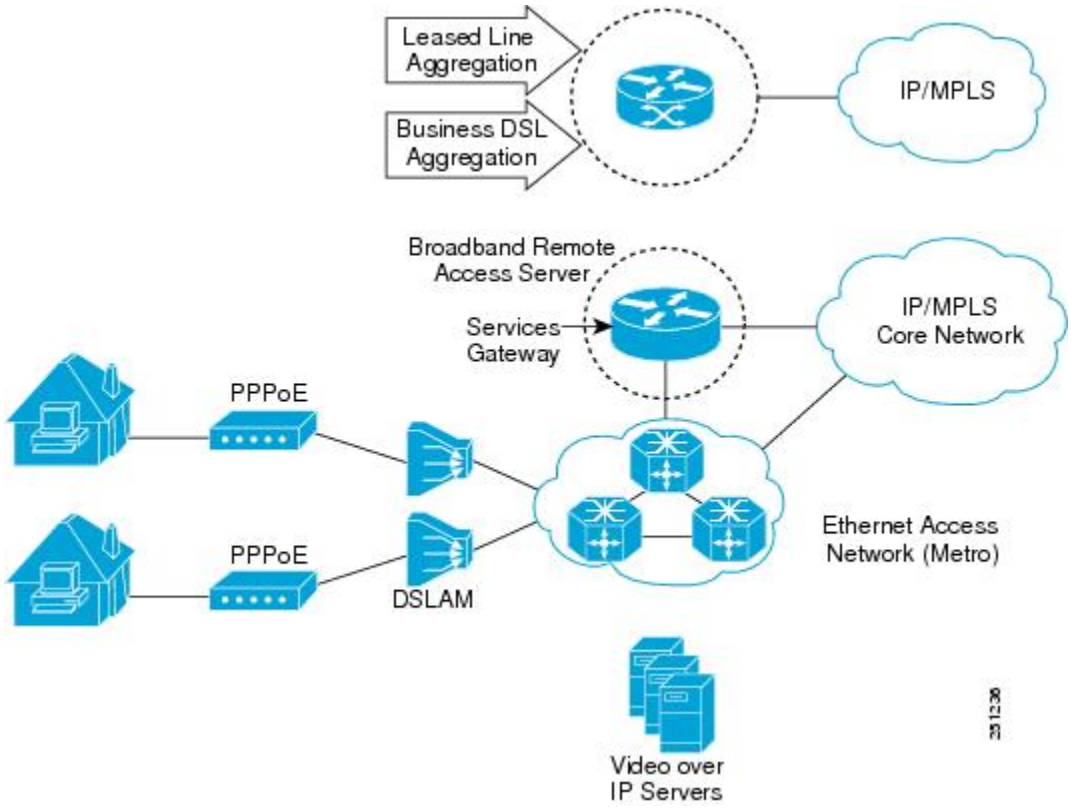
The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoE over VLAN, and PPPoE over QinQ sessions, during supported software upgrades, downgrades, and enhancements.

ISSU RA-MLPS VPN

The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPPoA and PPPoE (PPPoX) sessions terminated into remote access (RA)-Multiprotocol Label Switching (MPLS) VPN or PPPoX into MPLS VPN during supported software upgrades, downgrades, and enhancements.

The figure below shows a typical broadband aggregation HA deployment with ISSU functionality.

Figure 34: Broadband Aggregation High Availability Deployment



Benefits of Broadband High Availability In-Service Software Upgrade

- Eliminates network downtime for Cisco IOS XE software upgrades.
- Eliminates resource scheduling challenges associated with planned outages and late night maintenance windows.
- Accelerates deployment of new services and applications and allows faster implementation of new features, hardware, and fixes.
- Reduces operating costs due to outages while delivering higher service levels.
- Provides additional options for adjusting maintenance windows.
- Minimizes the impact of upgrades to service and allows for faster upgrades, resulting in higher availability.

How to Configure Broadband High Availability In-Service Software Upgrade

Configuring Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade

The Broadband High Availability In-Service Software Upgrade feature is enabled by default. This task configures subscriber redundancy policy for HA ISSU capability, allowing you to manage synchronization between HA active and standby processors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy** {**bulk limit**{**cpu percentage delay** *delay-time* [**allow value**] | **time** *seconds* | **delay** *delay-time* | **dynamic limit cpu percentage delay** *delay-time* [**allow value] | rate sessions time}**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**subscriber redundancy** {**bulk limit**{**cpu percentage delay** *delay-time* [**allow value**] | **time** *seconds* | **delay** *delay-time* | **dynamic limit cpu percentage delay** *delay-time* [**allow value] | rate sessions time}** **Example:** `Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`	(Optional) Configures subscriber redundancy policy.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA ISSU

To verify the subscriber redundancy policy configuration, use the **show running-config** command. Sample output is available in the Configuration Examples for Broadband High Availability In-Service Software Upgrade, on page 522.

- Step 1, Step 2 and Step 3 are useful for troubleshooting the CCM synchronization component.
- Step 4, Step 5 and Step 6 are useful for reviewing PPPoX session statistics.
- Step 7 and Step 8 are useful for verifying the failure of any L2TP tunnels or VPDN groups.
- Step 9 and Step 10 are typically used by Cisco engineers for internal debugging purposes.

SUMMARY STEPS

1. **show ccm clients**
2. **show ccm sessions**
3. **show ccm queues**
4. **show ppp subscriber statistics**
5. **show pppatm statistics**
6. **show pppoe statistics**
7. **show vpdn redundancy**
8. **show vpdn history failure**
9. **debug pppatm redundancy**
10. **debug pppoe redundancy**

DETAILED STEPS

Step 1 **show ccm clients**

This command displays information about the CCM, the HA component that manages the capability to synchronize session launch on the standby processor of a redundant processor HA system. Use the **show ccm clients** command to display information about CCM clients.

Example:

```
Router# show ccm clients
CCM bundles sent since peer up:
                                    Sent            Queued for flow control
    Sync Session                    0               0
    Update Session                  0               0
    Active Bulk Sync End            1               0
    Session Down                    0               0
    ISSU client msgs                350             0
    Dynamic Session Sync            0               0
    Unknown msgs                    0               0
Client events sent since peer up:
    PPP                             0
    PPPoE                           0
    VPDN FSP                        0
    AAA                             0
    PPP SIP                         0
    LTERM                           0
    AC                              0
    L2TP CC                         0
    SSS FM                          0
    IP SIP                          0
    IP IF                           0
    COA                             0
    Auto Svc                        0
    VPDN LNS                        0
```

Step 2 **show ccm sessions**

This command displays information about sessions managed by CCM.

Example:

```
Router# show ccm sessions

Global CCM state:                       CCM HA Active - Dynamic Sync
Global ISSU state:                      Compatible, Clients Cap 0x9EFFE
                                        Current     Bulk Sent   Bulk Rcvd
                                        ----------- ----------- -----------
Number of sessions in state Down:       0           0           0
Number of sessions in state Not Ready:  0           0           0
Number of sessions in state Ready:      0           0           0
Number of sessions in state Dyn Sync:   0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk CPU Lim 00:00:10 -         0           90        0
         Bulk Time Li 00:00:01 -         0           -         -
         RF Notif Ext 00:00:01 -         8           -         -
```

Step 3 **show ccm queues**

Use the **show ccm queues** command to display queue statistics for CCM sessions on active and standby processors. This command is primarily used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# show ccm queues
11 Event Queues
                size   max      kicks     starts    false   suspends  ticks(ms)
 3 CCM             0     8         82         83        1          0         20
 Event Names
                         Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  3 Sync Session            0       0          0         0         0       0
 2  3 Sync Client             0       0          0         0         0       0
 3  3 Update                  0       0          0         0         0       0
 4  3 Session Down            0       0          0         0         0       0
 5  3 Bulk Sync Begi          1       0          1         0         0       0
 6  3 Bulk Sync Cont          2       0          2         0         0       0
 7  3 Bulk Sync End           1       0          1         0         0       0
 8  3 Rcv Bulk End            0       0          0         0         0       0
 9  3 Dynamic Sync C          0       0          0         0         0       0
10  3 Going Active            0       0          0         0         0       0
11  3 Going Standby           0       0          0         0         0       0
12  3 Standby Presen          1       0          1         0         0       0
13  3 Standby Gone            0       0          0         0         0       0
15  3 CP Message            205       0          8         0       141    1000
16  3 Recr Session            0       0          0         0         0       0
17  3 Recr Update             0       0          0         0         0       0
18  3 Recr Sess Down          0       0          0         0         0       0
19  3 ISSU Session N          1       0          1         0         0       0
20  3 ISSU Peer Comm          0       0          0         0         0       0
21  3 Free Session            0       0          0         0         0       0
22  3 Sync Dyn Sessi          0       0          0         0         0       0
23  3 Recr Dyn Sessi          0       0          0         0         0       0
24  3 Session Ready           0       0          0         0         0       0
25  3 Pending Update          0       0          0         0         0       0
FSM Event Names           Events
 0    Invalid                 0
 1    All Ready               0
 2    Required Not Re         0
 3    Update                  0
 4    Down                    0
 5    Error                   0
 6    Ready                   0
 7    Not Syncable            0
 8    Recreate Down           0
```

Step 4 show ppp subscriber statistics

This command is useful for displaying events and statistics for PPP subscribers. Use the **show ppp subscriber statistics** command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the **clear ppp subscriber statistics** command was last issued.

Example:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       7             7
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
```

```
SSMDisc                       0            0
PPPDisc                       0            0
PPPBindResp                   7            7
PPPReneg                      3            3
RestartTimeout                5            5
PPP Subscriber Statistics     TOTAL        SINCE CLEARED
IDB CSTATE UP                 4            4
IDB CSTATE DOWN               8            8
APS UP                        0            0
APS UP IGNORE                 0            0
APS DOWN                      0            0
READY FOR SYNC                8            8
```

Step 5 **show pppatm statistics**

This command is useful for obtaining statistics for PPPoA sessions. Use the **show pppatm statistics** command to display a total count of PPPoA events since the **clear pppatm statistics**command was last issued.

Example:

```
Router# show pppatm statistics
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

Step 6 **show pppoe statistics**

This command is useful for obtaining statistics and events for PPPoE sessions. Use the **show pppoe statistics** command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the last time the **clear pppoe statistics** command was issued.

Example:

```
Router# show pppoe statistics
PPP Subscriber Events         TOTAL        SINCE CLEARED
Encap                         5            5
DeEncap                       2            2
CstateUp                      0            0
CstateDown                    0            0
FastStart                     0            0
LocalTerm                     0            0
LocalTermVP                   0            0
MoreKeys                      0            0
Forwarding                    0            0
Forwarded                     0            0
SSSDisc                       0            0
SSMDisc                       0            0
PPPDisc                       0            0
PPPBindResp                   0            0
PPPReneg                      0            0
RestartTimeout                2            2
PPP Subscriber Statistics     TOTAL        SINCE CLEARED
```

```
IDB CSTATE UP                  0             0
IDB CSTATE DOWN                0             0
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 0             0
ASR1006-1#sh pppoe statis
ASR1006-1#sh pppoe statistics ?
  |  Output modifiers
  <cr>
ASR1006-1#sh pppoe statistics
PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              0             0
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
SSS DISCONNECT ACK             0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM ACCT STATS UPDATED         0             0
SSM DISCONNECT                 0             0
                               0             0
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        0             0
PPPoE Handles Freed            0             0
Dynamic Bind Request           0             0
Static Bind Request            0             0
SSM Async Stats Request        0             0
```

Step 7 show vpdn redundancy

Use this command to verify the failure of any L2TP tunnels.

Example:

```
Router# show vpdn redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    0
  L2TP Tunnels:            0/0/0/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           0/0/0 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   0/0 (success/fail)
```

Step 8 show vpdn history failure

Use this command to verify the failure of any VPDN groups.

Example:

```
Router# show vpdn history failure

% VPDN user failure table is empty
```

Step 9 **debug pppatm redundancy**

Use the **debug pppatm redundancy** command to display CCM events and messages for PPPoA sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppatm redundancy
*Dec  3 02:58:40.784: PPPATM HA: [14000001]: Received the first SHDB
*Dec  3 02:58:40.784: PPPATM HA: [14000001]: Base hwidb not created > yet, queuing SHDB *Dec  3
02:58:40.784: PPPATM HA: [14000001]:
Requesting base vaccess creation
```

Step 10 **debug pppoe redundancy**

Use the **debug pppoe redundancy** command to display CCM events and messages for PPPoE sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppoe redundancy
Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

Configuration Examples for Broadband High Availability In-Service Software Upgrade

Example Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade

The following example shows how to configure the Broadband High Availability In-Service Software Upgrade feature:

```
enable
configure terminal
subscriber redundancy bulk limit cpu 75 delay 20 allow 30
end
```

The following is a sample configuration of PPPoX terminated into an RA-MPLS network with SSO. Commands that appear in the configuration task tables for this feature but that do not appear in the running configuration output are configured for their default settings.

```
hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

The following lines show subscriber redundancy policy configuration:

```
subscriber redundancy dynamic limit cpu 90 delay 10
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
buffers small permanent 15000
buffers middle permanent 12000
buffers large permanent 1000
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
```

```
  virtual-template 2
!
bba-group pppoe grp3
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 172.16.1.1 255.255.255.255
!
interface Loopback100
  ip address 172.31.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
encapsulation dot1Q 2
pppoe enable group grp2
!
!
interface GigabitEthernet1/0/1
no ip address
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
```

```
encapsulation dot1Q 2
pppoe enable group grp5
!
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
!
interface GigabitEthernet7/0/3
no ip address
!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
```

```
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
  network 10.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 10.0.0.3 remote-as 1
  neighbor 10.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 send-community extended
  exit-address-family
  !
```

```
  address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.1.1.1 10.1.16.160
ip local pool pool4 10.1.1.1 10.1.16.160
ip local pool pool5 10.1.1.1 10.1.16.160
ip local pool pool6 10.1.1.1 10.1.16.160
ip local pool pool7 10.1.1.1 10.1.16.160
ip local pool pool8 10.1.1.1 10.1.16.160
ip classless !
!
no ip http server
!
!
arp 10.1.1.1 0020.0001.0001 ARPA
arp vrf vrf1 10.1.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Broadband commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference
High Availability	"High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide
Performing an ISSU	The following chapters in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide : • "Cisco IOS XE Software Package Compatibility for ISSU" • "In Service Software Upgrade (ISSU)"
Broadband SSO	Broadband High Availability Stateful Switchover
Stateful switchover	Stateful Switchover
Cisco nonstop forwarding	Cisco Nonstop Forwarding
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

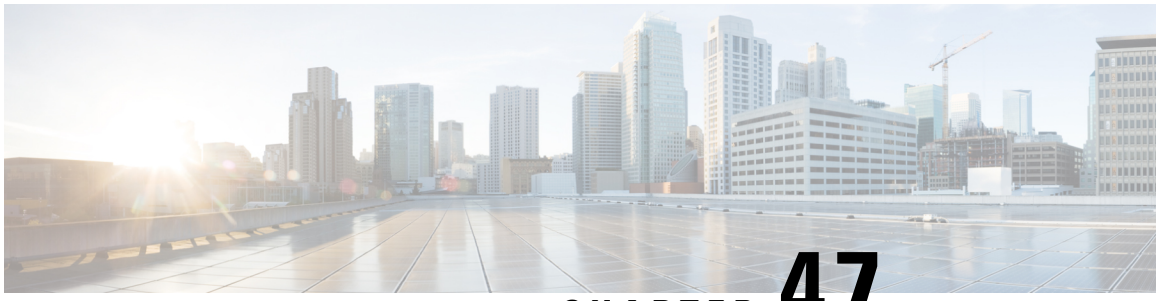
Feature Information for Broadband High Availability In-Service Software Upgrade

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 55: Feature Information for Cisco IOS Broadband High Availability In-Service Software Upgrade

Feature Name	Releases	Feature Information
ISSU-PPPoA	Cisco IOS XE Release 3.3S	This feature was introduced on Cisco ASR 1000 Series Routers. This feature uses the ISSU support for PPPoA to ensure continuous operations of broadband access protocols during software upgrades. The following commands were introduced or modified: **debug pppatm redundancy** , **debug pppoe redundancy**, **show pppoe redundancy**, **show pppatm redundancy**, **show pppatm statistics**, **subscriber redundancy**
ISSU--PPPoE	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Routers. This feature uses the ISSU--PPPoE support to ensure continuous operations of broadband access protocols during software upgrades, downgrades, and service enhancements. The following commands were introduced or modified: **clear ppp subscriber statistics**, **clear pppoe statistics**, **debug pppoe redundancy, show ccm clients, show ccm sessions, show ppp subscriber statistics, show pppoe statistic, subscriber redundancy**



CHAPTER 47

Controlling Subscriber Bandwidth

The Dynamic Subscriber Bandwidth Selection (DBS) feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM quality of service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session is established.

Prerequisites for Controlling Subscriber Bandwidth

A Cisco ASR 1000 series router must have the following shared port adapters (SPAs) installed to enable DBS:

- SPA-3XOC3-ATM-V2
- SPA-1XOC3-ATM-V2
- SPA-1XOC12-ATM-V2

Restrictions for Controlling Subscriber Bandwidth

The DBS feature does not support the following:

- Switched virtual circuits (SVC)
- ATM port adapters installed in a Cisco ASR 1000 series router
- When changing QoS values dynamically on a VC, there can be some duration (in milliseconds) during which traffic on the VC is dropped.

Information About Controlling Subscriber Bandwidth

Traffic-Shaping Parameters

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic-shaping parameters to be dynamically changed based on the RADIUS profile of a PPPoE or PPPoA user logging in on the PVC. If the user is the first user on a given PVC, the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all the sessions are selected as the PCR and SCR, respectively, of the VC.

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Traffic-shaping parameters can be locally configured by Cisco IOS command-line interface (CLI) in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic-shaping parameters that are CLI-configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overridden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a "QoS-management" string via vendor-specific attribute (VSA) 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for a particular user or domain. If the QoS specified for a domain or user cannot be applied on the PVC to which the session belongs, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** command to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you configure the **no dbs enable** command on a VC, additional sessions that are configured will display DBS-configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessions are already up on the VC, all sessions on that VC have DBS QoS parameters.

Benefits of Controlling Subscriber Bandwidth

DBS provides the following benefits:

- Wholesale service providers can provide different bandwidth options to their retail service provider customers, such as ISPs and enterprises.
- Subscribers can choose between enhanced and basic service, with a fixed billing plan for each service.

How to Control Subscriber Bandwidth

Configuring DBS Under a VC Class

Perform the following task to configure DBS under a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **dbs enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm class1`	Creates an ATM VC class and enters ATM VC class configuration mode. • A VC class can be applied to an ATM interface, subinterface, or VC.
Step 4	**dbs enable** **Example:** `Router(config-vc-class)# dbs enable`	Applies DBS QoS parameters.

Configuring DBS on a PVC

Perform the following task to configure DBS for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]

4. **pvc** [*name*] *vpi /vci*
5. **dbs enable**
6. **protocol pppoe**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**pvc** [*name*] *vpi /vci* **Example:** `Router(config-if)# pvc 2/101`	Specifies an ATM PVC and creates or assigns a name to an ATM PVC, and enters interface-ATM-VC configuration mode. **Note** The arguments *vpi* and *vci* cannot both be set to 0; if one is 0, the other cannot be 0.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Applies DBS QoS parameters.
Step 6	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Specifies PPPoE as the protocol of the ATM PVC.

Configuring DBS on a Range of PVCs

Perform this task to configure DBS for a range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]

4. **range**[*range-name*] **pvc** *start-vpi* / *start-vci end-vpi /end-vci*
5. **dbs enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**range**[*range-name*] **pvc** *start-vpi* / *start-vci end-vpi /end-vci* **Example:** `Router(config-subif)# range pvc 0/101 0/500 class-range pppoe`	Defines a range of ATM PVCs and enables PVC range configuration mode.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Applies DBS QoS parameters.

Configuring DBS on a PVC Within a PVC Range

Perform this task to configure DBS for a specific PVC within a range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **in-range** [*pvc-name*] [[*vpi* /]*vci*]
6. **dbs enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 0/101 0/500 class-range pppoe`	Defines a range of ATM PVCs and enables PVC range configuration mode.
Step 5	**in-range** [*pvc-name*] [[*vpi* /]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.
Step 6	**dbs enable** **Example:** `Router(config-if-atm-range-pvc)# dbs enable`	Applies DBS QoS parameters.

Configuring the RADIUS Attributes for DBS

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Configure the RADIUS attributes listed in this section in the user or domain profiles on the authentication, authorization, and accounting (AAA) server. The user or domain profile is downloaded from the AAA server as part of user authentication.

The QoS management string for DBS has the following syntax:

```
Cisco-Avpair = atm:peak-cell-rate=155000
Cisco-Avpair = atm:sustainable-cell-rate=155000
```

You must configure the PCR. Configuring the SCR is optional. If you configure only the PCR, the ATM service type is an unspecified bit rate (UBR). If you specify both the SCR and the PCR, the ATM service type is a variable bit rate nonreal-time (VBR-nrt) connection.

If the peak rate is greater than the maximum rate permitted on the ATM physical interface, the PCR applied on the ATM PVC is set to the maximum rate. If the specified PCR is less than the minimum rate, then the PCR applied on the ATM PVC is the minimum rate.

If the sustainable-cell-rate (in Kbps) applied exceeds the maximum for the interface, the session is rejected.

Note DBS cannot change service categories such as from UBR to VBR-nrt. For details, see the table in Configuring Dynamic Suscriber Services .

Verifying DBS

Note The configuration examples in this section explain the PPPOE termination using a VPDN group.

SUMMARY STEPS

1. Enter the **show atm pvc** *vpi* / *vci*command to view details about ATM PVCs or VCs:
2. Enter the **show atm pvc dbs**command to display information about ATM PVCs that have DBS QoS parameters applied:
3. Enter the **show running-config** command to verify that DBS QoS parameters have been applied. If you enter the **dbs enable** or the **no dbs enable**command, it appears in the output of the **show running-config command**. If you enter the **default dbs enable**command, it does not appear.

DETAILED STEPS

Step 1 Enter the **show atm pvc** *vpi* / *vci*command to view details about ATM PVCs or VCs:

Example:

```
Router# show atm pvc 0/75
ATM1/0.4:VCD:1, VPI:0, VCI:75
UBR, PeakRate:149760
AAL5-LLC/SNAP, etype:0x0, Flags:0xC20, VCmode:0x0
OAM frequency:0 second(s), OAM retry frequency:1 second(s)
OAM up retry count:3, OAM down retry count:5
OAM Loopback status:OAM Disabled
OAM VC state:Not Managed
ILMI VC state:Not Managed
PA TxRingLimit:40 particles
PA Rx Limit:1600 particles
InARP frequency:15 minutes(s)
Transmit priority 4
```

```
InPkts:18, OutPkts:21, InBytes:1263, OutBytes:1476
InPRoc:18, OutPRoc:3
InFast:0, OutFast:0, InAS:0, OutAS:0
InPktDrops:0, OutPktDrops:0/0/0 (holdq/outputq/total)
CrcErrors:0, SarTimeOuts:0, OverSizedSDUs:0, LengthViolation:0,
CPIErrors:0
Out CLP=1 Pkts:0
OAM cells received:0
F5 InEndloop:0, F5 InSegloop:0, F5 InAIS:0, F5 InRDI:0
F4 InEndloop:0, F4 InSegloop:0, F4 InAIS:0, F4 InRDI:0
OAM cells sent:0
F5 OutEndloop:0, F5 OutSegloop:0, F5 OutRDI:0
F4 OutEndloop:0, F4 OutSegloop:0, F4 OutRDI:0
OAM cell drops:0
Status:UP
PPPOE enabled.
DBS enabled.
```

Step 2 Enter the **show atm pvc dbs**command to display information about ATM PVCs that have DBS QoS parameters applied:

Example:

```
Router# show atm pvc dbs
            VCD /                                       Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells
Sts
1/0.7      3            0    75   PVC    MUX      VBR    2000    700   94
UP
```

Step 3 Enter the **show running-config** command to verify that DBS QoS parameters have been applied. If you enter the **dbs enable** or the **no dbs enable**command, it appears in the output of the **show running-config command**. If you enter the **default dbs enable**command, it does not appear.

Example:

```
Router# show running-config
Building configuration...
Current configuration : 2902 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa session-id common
!
username usera password 0 password0
username lac password 0 password1
username lns password 0 password2
username nrp1 password 0 password3
username user1 password 0 password4
username nrp1-3 password 0 password5
username xyz@abc.com password 0 password6
ip subnet-zero
!
```

```
!
ip host dirt 172.69.1.129
ip host boot 172.19.192.254
!
vpdn enable
!
vpdn-group lac
 request-dialin
  protocol l2f
  domain pepsi.com
 initiate-to ip 10.1.1.5
 local name lac
!
vpdn-group pppoe_terminate
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 2000
 pppoe limit per-vc 2000
!
!
!
!
!
!
!
!
!
vc-class atm pppoa
  encapsulation aal5mux ppp Virtual-Template2
  dbs enable
!
vc-class atm pppoe
  dbs enable
  protocol pppoe
!
interface Loopback1
 no ip address
!
interface FastEthernet0/0
 ip address 10.0.74.211 255.255.255.0
 duplex half
 no cdp enable
!
interface ATM1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
!
interface ATM1/0.4 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 pvc 0/75
  dbs enable
  protocol pppoe
 !
!
interface ATM1/0.5 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
```

```
 pvc 0/85
 !
!
interface ATM1/0.7 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 pvc 0/95
  class-vc pppoa
  ubr 5000
 !
!
interface ATM1/0.10 point-to-point
 no ip route-cache
 no ip mroute-cache
 range pvc 0/101 0/500
  class-range pppoe
 !
  pvc-in-range 0/102
   no dbs enable
  !
!
interface Virtual-Template1
 ip unnumbered Loopback1
 ip mtu 1492
 no keepalive
 peer default ip address pool local_pool
 ppp authentication chap
!
interface Virtual-Template2
 ip address negotiated
 ip mtu 1492
 peer default ip address pool local_pool
 ppp authentication chap
!
interface Virtual-Template10
 ip address 192.168.11.1 255.255.255.0
 no keepalive
 peer default ip address pool p3
 ppp authentication chap
!
interface Virtual-Template11
 ip address negotiated
 no keepalive
 ppp chap hostname host1
 ppp chap password password1
!
ip local pool p3 192.168.0.0 192.170.12.250
ip local pool local_pool 150.10.3.1 150.10.10.250
ip default-gateway 10.0.74.1
ip classless
ip route 10.0.0.0 10.0.0.0 10.0.74.1
ip route 10.107.164.0 255.255.255.0 FastEthernet0/0
no ip http server
!
!
!
radius-server host 172.18.0.0 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
!
mgcp profile default
```

```
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 5 15
!
!
end
```

Monitoring DBS

Use the commands listed below to monitor DBS:

Command	Purpose
debug atm events	Displays the normal set of ATM events when a session comes up or goes down.
debug atm errors	Displays protocol errors and error statistics associated with VCs.
debug atm status	Displays changes in the status of a VC when a session comes up or goes down or when the VC configuration is changed.
debug ppp authentication	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
debug ppp error	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
debug ppp negotiation	Enables debugging of PPP negotiation process.
debug radius	Displays detailed debugging information associated with RADIUS.
debug vpdn event	Displays Layer 2 tunneling protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
debug vpdn l2x-errors	Displays Layer 2 forwarding protocol (L2F) and L2TP errors that prevent tunnel establishment or normal operation.
debug vpdn 12x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
show atm pvc	Displays all ATM PVCs and traffic information.

Command	Purpose
show atm pvc dbs	Displays ATM PVCs that have DBS QoS parameters applied.
show atm vc detailed	Displays information about ATM PVCs and SVCs.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.

Configuration Examples for Controlling Subscriber Bandwidth

Configuring DBS for a VC Class Example

In the following example, DBS QoS parameters have been applied to a VC called "cisco":

```
vc-class atm cisco
 dbs enable
```

Configuring DBS for a PVC Example

In the following example, DBS QoS parameters have been applied on a PVC called "cisco":

```
interface atm0/0/0.5 point-to-point
 ip address 10.0.0.0 255.255.255.0
 pvc cisco 0/100
 dbs enable
 protocol pppoe
```

Configuring DBS for a Range of PVCs Example

In the following example, DBS QoS parameters have been applied on a range of PVCs. The range is named "cisco range" and has a *start-vpi* of 0, a *start-vci* of 50, an *end-vpi*of 0, and an *end-vci* of 70:

```
interface atm0/0/0.1 multipoint
 ip address 10.0.0.0 255.255.255.0
 range cisco pvc 0/50 0/70
 dbs enable
```

Configuring DBS for a PVC Within a PVC Range Example

In the following example, DBS parameters have been applied on PVC 60, which is part of the PVC range called "cisco":

```
interface atm0/0/0.1 multipoint
 range cisco pvc 0/50 0/70
 pvc-in-range 0/60
 dbs enable
```

Configuring RADIUS Attributes Examples

The following example shows how to configure RADIUS attributes for a domain profile for DBS:

```
cisco.com  Password = "cisco", Service-Type = Outbound
     Service-Type = Outbound,
     Cisco-Avpair = "vpdn:tunnel-id=tunnel33",
     Cisco-Avpair = "vpdn:tunnel-type=l2tp",
     Cisco-Avpair = "vpdn:l2tp-tunnel-password=password2",
     Cisco-Avpair = "vpdn:ip-addresses=172.16.0.0",
     Cisco-Avpair = "atm:peak-cell-rate=155000",
     Cisco-Avpair = "atm:sustainable-cell-rate=155000"
```

The following example shows how to configure RADIUS attributes for a user profile for DBS:

```
user1@cisco.com Password = "userpassword1", Service-Type = Outbound
     Service-Type = Outbound,
     Cisco-Avpair = "atm:peak-cell-rate=155000",
     Cisco-Avpair = "atm:sustainable-cell-rate=155000"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco Subscriber Edge Services Manager	Cisco Subscriber Edge Services Manager
Access Point Name Manager	APN Manager Application Programming Guide
RADIUS configuration	*"Configuring RADIUS" chapter of the Cisco IOS Security Configuration Guide*
RADIUS attributes	"RADIUS Attributes" appendix to the *Cisco IOS Security Configuration Guide*
Broadband access aggregation concepts	*"* Understanding Broadband Access Aggregation*" module*
Tasks for preparing for broadband access aggregation	*"* Preparing for Broadband Access Aggregation*" module*
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	"Wide-Area Networking Commands" in the *Cisco IOS Wide-Area Networking Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

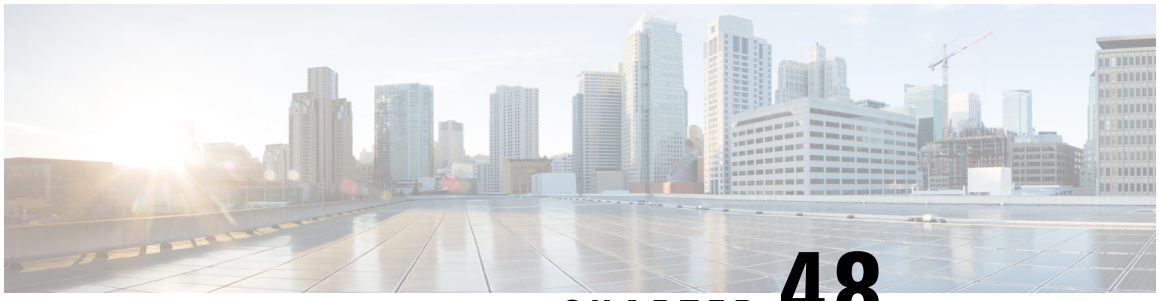
Feature Information for Controlling Subscriber Bandwidth

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 56: Feature Information for Controlling Subscriber Bandwidth

Feature Name	Releases	Feature Configuration Information
Dynamic Subscriber Bandwidth Selection (DBS)	Cisco IOS XE Release 2.5	This feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM quality of service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.



CHAPTER 48

PPPoE Service Selection

The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. You choose one of the services offered, and the service is provided when the PPPoE session becomes active. This feature enables service providers to offer a variety of services and to charge you according to the service chosen.

Prerequisites for PPPoE Service Selection

- PPPoE must be configured using PPPoE profile configuration rather than virtual private dial-up network (VPDN) group configuration as described in the "Providing Protocol Support for Broadband Aggregation of PPPoE Sessions" module.
- The PPPoE client must support service tags in the PPPoE discovery phase.
- The procedures in this document assume that RADIUS accounting and authentication, and PPPoE are configured and working, if you use PPPoE service selection to offer tunneling services.
- You must configure either the **subscriber authorization enable** or the **vpdn enable** command before configuring PPPoE service selection to successfully create service names.

Information About PPPoE Service Selection

PPPoE Service Selection Through Service Tags

PPPoE service selection enables a PPPoE server to offer clients a selection of services during call setup. The PPPoE client chooses one of the services offered, and that service is provided when the PPPoE session becomes active.

PPPoE service selection works through the exchange of service tags during the PPPoE discovery phase. When a client initiates a call with a PPPoE Active Discovery Initiation (PADI) packet, the PPPoE server responds with a PPPoE Active Discovery Offer (PADO) packet that advertises a list of available services. The client selects a service and sends a PPPoE Active Discovery Request (PADR) packet that indicates the service name that was selected.

When the PPPoE server receives the PADR packet that indicates the chosen service, the PPPoE server handles the service name in the same manner as a domain name. The service profile for the service name is retrieved from a RADIUS server, and the attributes within that service profile are applied to the call.

PPPoE Service Names

Each PPPoE service has a service name, which can be defined as a set of characteristics that are applied to a PPPoE connection when that service name is selected during call setup.

When you configure PPPoE service selection, you can define a RADIUS service profile for each service name, list in a subscriber profile the service names that you want to advertise, and then assign the subscriber profile to a PPPoE profile. The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

If a subscriber profile is not assigned to a PPPoE profile, the PPPoE connections that use that PPPoE profile are established without the additional service tags in the discovery packets. If a port is configured with a static service name (using the **vpn service** command), the static service name takes precedence, and no services are advertised to the client.

The Cisco RADIUS vendor-specific attribute (VSA) "service-name" is used in RADIUS accounting records to log the service name that was selected by the client. This attribute is also used to download the service names from the subscriber profile when the subscriber profile is defined on the RADIUS server.

You can use the **pppoe-client dial-pool-number** command to configure a PPPoE client. While configuring the PPPoE client, you can also specify the service name requested by the PPPoE client. This service name allows the PPPoE client to signal a service name to the Broadband Access Aggregation System (BRAS). By default, no service name is signaled and the service name value is set to NULL.

A single Permanent Virtual Connection (PVC) can support multiple PPPoE clients and redundancy. You can use the **pppoe-client dial-pool-number** command to configure one or more concurrent client PPPoE sessions on a single Asynchronous Transfer Mode (ATM) PVC.

RADIUS Service Profiles for PPPoE Service Selection

A service profile must be created on the RADIUS server for each service name. The service profile contains attributes that define how the call is handled. Currently, two sets of attributes are available for defining service profiles: attributes that define tunneling and attributes that define the quality of service (QoS) that is applied to the permanent virtual circuit (PVC) on which the PPPoE call is coming in.

The table below lists some of the attributes that are supported in RADIUS service profiles for PPPoE service selection.

Benefits of PPPoE Service Selection

PPPoE service selection enables a service provider to use PPPoE to offer a selection of services to you and to charge you according to the service selected. For example, a wholesaler could offer different levels of

service by defining multiple service profiles for the same tunnel but with different levels of QoS for the ATM PVC. The wholesaler would be able to charge you according to the level of service provided.

PPPoE service selection could also be used by access providers to avoid link control protocol (LCP) negotiation at the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) for sessions that are to be forwarded to tunnels. Avoiding LCP negotiation at the LAC can improve scalability of the LAC during call setup and help alleviate the load on the LAC while all the sessions on the LAC are reconnecting after an outage.

Attributes Used to Define a RADIUS Service Profile for PPPoE Selection

The table below lists some of the attributes that can be used to define a RADIUS service profile for PPPoE service selection. These attributes are defined when setting up the RADIUS server.

Table 57: Attributes for the RADIUS Service Profile for PPPoE Service Selection

RADIUS Entry	Purpose
User-Service-Type = Outbound-User	Configures the service type as outbound.
Cisco-AVpair = "vpdn:tunnel-id= *name* **"**	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.
Cisco-AVpair = "vpdn:tunnel-type=l2tp"	Specifies Layer 2 Tunnel Protocol (L2TP).
Cisco-AVpair = "vpdn:ip-addresses= *ip-address* **"**	Specifies the IP address of L2TP network server (LNS).
Cisco-AVpair = "atm:peak-cell-rate= *kbps* **"**	Specifies the peak cell rate, in kbps, that is applied to the ATM PVC on which a PPPoE session is being established.
Cisco-AVpair = "atm:sustainable-cell-rate= *kbps* **"**	Specifies the sustainable cell rate, in kbps, that is applied to the ATM PVC on which a PPPoE session is being established.

Attributes Used to Configure a Subscriber Profile on the RADIUS Server for PPPoE Service Selection

The table below lists the attributes that can be used to configure a RADIUS subscriber profile to support PPPoE service selection.

The default AAA authorization method list determines where the policy manager looks for the subscriber profile. When the subscriber profile is configured remotely, the **aaa authorization network default group radius**command must be included in the AAA configuration so the policy manager knows to look for the subscriber policy on a AAA server. These attributes are defined while configuring the RADIUS server. Refer to the RADIUS server documentation for information about how to perform this configuration.

Table 58: Attributes for the RADIUS Subscriber Profile for PPPoE Service Selection

RADIUS Entry	Purpose
`User-Service-Type = Outbound-User`	Configures the service type as outbound.
`Cisco-AVpair = "pppoe:service-name=`*`service-name`*`"`	Specifies a PPPoE service name that is listed in this subscriber profile.

How to Offer PPPoE Service Selection

Configuring the Subscriber Profile for PPPoE Service Selection

The subscriber profile contains the list of services that is advertised to PPPoE clients. You can configure the subscriber profile locally on the router or on the RADIUS server.

If the services are defined locally and the subscriber services points to RADIUS server, the PPPoE services must come from RADIUS which is not been defined, empty, or unavailable for specific reason. You can configure either the **subscriber authorization enable** or the **vpdn enable** command before configuring PPPoE service selection to successfully create service names.

Perform this task to configure a local subscriber profile for PPPoE service selection.

Before you begin

The default AAA authorization method list determines where the policy manager looks for the subscriber profile. When the subscriber profile is configured locally, the **aaa authorization network default local** command must be included in the AAA configuration so the policy manager knows to look for the subscriber policy locally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **pppoe service** *service-name*
5. Repeat Step 4 for each service name that you want to add to the subscriber profile.
6. **end**
7. end

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service abc`	Enters service policy map configuration mode and creates or modifies a service policy map, which is used to define an Intelligent Services Gateway (ISG) subscriber service.
Step 4	**pppoe service** *service-name* **Example:** `Router(config-service-policymap)# pppoe service gold-isp-A`	Adds a PPPoE service name to a subscriber profile.
Step 5	Repeat Step 4 for each service name that you want to add to the subscriber profile.	--
Step 6	**end** **Example:** `Router(config-service-policymap)# end`	(Optional) Terminates the configuration session and returns to global configuration mode.
Step 7	end **Example:** `Router(config)# end`	(Optional) Exits global configuration mode.

Configuring the PPPoE Profile for PPPoE Service Selection

Perform this task to associate a subscriber profile with a PPPoE profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-vc limit** *number*
6. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
7. **end**
8. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group1`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template is used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions per-vc limit** *number*	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile.
Step 6	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Router(config-bba-group)# service profile subscriber-group1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. • The PPPoE configuration that is derived from the subscriber gold_isp_A (where gold services created using the Cisco Distributed Administrative Tool (CDAT) interface are defined) under the PPPoE profile. Use the **service profile** command with the **refresh** keyword and the *minutes* argument to cause the cached PPPoE configuration to be timed out after a specified number of minutes.
Step 7	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Returns to global configuration mode.
Step 8	end **Example:**	(Optional) Exits global configuration mode.

	Command or Action	Purpose
	`Router(config)# end`	

Troubleshooting Tips

Use the **show pppoe session** and **debug pppoe** commands to troubleshoot PPPoE sessions.

What to Do Next

Once a PPPoE profile has been defined, it must be assigned to a PPPoE port (Fast Ethernet, virtual LAN [VLAN], or PVC), a virtual circuit (VC) class, or an ATM PVC range. For more information about how to configure PPPoE profiles, refer to the Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions chapter.

Configuring Service Names for PPPoE Clients on an ATM PVC

Perform this task to configure the service name for PPPoE client on an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe-client dial-pool-number** *number* **restart** *number* **service-name** *name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Configures an ATM interface.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:**	Creates an ATM PVC and enters ATM virtual circuit configuration.

	Command or Action	Purpose
	`Router(config-if)# pvc 1/100`	
Step 5	**pppoe-client dial-pool-number** *number* **restart** *number* **service-name** *name* **Example:** `Router(config-if-atm-vc)# pppoe-client dial-pool-number 1 restart 80 service-name "test 4"`	Configures the PPPoE client, specifies the dialer interface number, restart number, and service name to use for cloning on the PVC. **Note** • The dial-pool number is the number that is assigned to a configured dialer pool. The range is from 1 to 255. • The restart number is the timer configured in seconds. The range is from 1 to 3600 and default value is 20. • The name indicates the service-name requested by the PPPoE client. The service name allows the PPPoE client to signal a service name to the Broadband Access Aggregation System (BRAS). By default, no service name is signaled and the service name value is set to NULL.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Returns to privileged EXEC mode.

What to do next

Note If you make any changes to the PVC configuration after the PPPoE client session is established, the session is automatically terminated and reestablished.

Verifying PPPoE Service Selection

Perform this task to verify PPPoE service selection configuration and performance. Steps 2 through 3 are optional and do not have to be performed in a particular order.

SUMMARY STEPS

1. **show pppoe derived group** *group-name*
2. **show vpdn** [**session** [**all** | **packets** | **sequence** | **state**] | **tunnel** [**all** | **packets** | **summary** | **state** | **transport**]]
3. **show atm pvc** [*vpi* / *vci* | *name* | **interface atm** *slot*/*subslot*/*port*[**.** *subinterface* **multipoint**]] [**ppp**]

DETAILED STEPS

Step 1 **show pppoe derived group** *group-name*

(Optional) Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.

This command is useful for viewing the subscriber profile configuration when the subscriber profile is configured on a remote AAA server.

Example:

```
Router# show pppoe derived group sp-group-a
Derived configuration from subscriber profile 'abc':
Service names:
   isp-xyz, gold-isp-A, silver-isp-A
```

Step 2 **show vpdn** [**session** [**all** | **packets** | **sequence** | **state**] | **tunnel** [**all** | **packets** | **summary** | **state** | **transport**]]

(Optional) Displays information about active L2TP or Layer 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN.

Use this command to display tunneling parameters for the services configured for tunneling.

Example:

```
Router# show vpdn
Active L2F tunnels
NAS Name   Gateway Name    NAS CLID   Gateway CLID   State
nas        gateway           4            2          open
L2F MIDs
Name                NAS Name    Interface    MID      State
router1@cisco.com       nas          As7          1       open
router2@cisco.com        nas          As8          2       open
```

Step 3 **show atm pvc** [*vpi* / *vci* | *name* | **interface atm** *slot*/*subslot*/*port*[**.** *subinterface* **multipoint**]] [**ppp**]

(Optional) Displays all ATM PVCs and traffic information.

Use this command to display ATM QoS parameters for the services configured for ATM QoS.

Example:

```
Router# show atm pvc
           VCD/                                    Peak      Avg/Min   Burst
Interface  Name   VPI   VCI   Type   Encaps       Kbps         Kbps   Cells      Sts
2/0        1        0     5    PVC     SAAL    155000       155000               UP
2/0        2        0    16    PVC     ILMI    155000       155000               UP
2/0.2      101      0    50    PVC     SNAP    155000       155000               UP
2/0.2      102      0    60    PVC     SNAP    155000       155000             DOWN
2/0.2      104      0    80    PVC     SNAP    155000       155000               UP
2/0        hello    0    99    PVC     SNAP      1000
```

Monitoring and Maintaining PPPoE Service Selection

To monitor and maintain PPPoE service selection, perform the following steps.

SUMMARY STEPS

1. **clear pppoe derived group** *group-name*
2. **debug pppoe events** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
3. **debug radius** [**brief** | **hex**]

DETAILED STEPS

Step 1 **clear pppoe derived group** *group-name*

Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.

Example:

```
Router# clear pppoe derived group group1
```

Step 2 **debug pppoe events** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

(Optional) Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.

Use this command to monitor the exchange of PPPoE service names during call setup.

Example:

```
Router# debug pppoe events interface atm 0/0.0 vc 101

PPPoE protocol events debugging is on
Router#
00:41:55:PPPoE 0:I PADI  R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101 ATM0/1/0.10
00:41:55:PPPoE 0:O PADO, R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:PPPoE 0:I PADR  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:PPPoE :encap string prepared
00:41:55:[3]PPPoE 3:Access IE handle allocated
00:41:55:[3]PPPoE 3:pppoe SSS switch updated
00:41:55:[3]PPPoE 3:AAA unique ID allocated
00:41:55:[3]PPPoE 3:No AAA accounting method list
00:41:55:[3]PPPoE 3:Service request sent to SSS
00:41:55:[3]PPPoE 3:Created  R:0001.c9f0.0c1c L:00b0.c2e9.c470 0/101 ATM0/1/0.10
00:41:55:[3]PPPoE 3:State REQ_NASPORT    Event MORE_KEYS
00:41:55:[3]PPPoE 3:O PADS  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:[3]PPPoE 3:State START_PPP    Event DYN_BIND
00:41:55:[3]PPPoE 3:data path set to PPP
00:41:57:[3]PPPoE 3:State LCP_NEGO    Event PPP_LOCAL
00:41:57:PPPoE 3/SB:Sent vtemplate request on base Vi2
00:41:57:[3]PPPoE 3:State CREATE_VA    Event VA_RESP
00:41:57:[3]PPPoE 3:Vi2.1 interface obtained
00:41:57:[3]PPPoE 3:State PTA_BIND    Event STAT_BIND
00:41:57:[3]PPPoE 3:data path set to Virtual Acess
00:41:57:[3]PPPoE 3:Connected PTA
```

Step 3 **debug radius** [**brief** | **hex**]

(Optional) Displays information associated with RADIUS.

Use this command to monitor the transactions between the router and the RADIUS server.

Example:

```
Router# debug radius

Radius protocol debugging is on
Radius packet hex dump debugging is off
Router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.0:0000, Accounting-Request, len
358
00:02:50: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:02:50: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS:  NAS-Port-Type       [61]  6   Async
00:02:50: RADIUS:  User-Name           [1]   12  "5559999999"
00:02:50: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:02:50: RADIUS:  Calling-Station-Id  [31]  12  "5559999999"
00:02:50: RADIUS:  Acct-Status-Type    [40]  6   Start
00:02:50: RADIUS:  Service-Type        [6]   6   Login
00:02:50: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:02:50: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS:  Vendor, Cisco       [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:02:50: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS:  Acct-Session-Id     [44]  10  "55559999"
00:02:50: RADIUS:  Delay-Time          [41]  6   0
00:02:51: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 5559000000
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 0.0.000.0:0000, Access-Request, len
171
00:03:01: RADIUS:  NAS-IP-Address      [4]   6   10.x.y.z
00:03:01: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:01: RADIUS:  User-Name           [1]   8   "123456"
00:03:01: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:01: RADIUS:  Calling-Station-Id  [31]  12  "555999999"
00:03:01: RADIUS:  User-Password       [2]   18  *
00:03:01: RADIUS:  Vendor, Cisco       [26]  36  VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 0 0.0.000.0 1:1823, Access-Accept, len 115
00:03:01: RADIUS:  Service-Type        [6]   6   Login
00:03:01: RADIUS:  Vendor, Cisco       [26]  29  VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS:  Vendor, Cisco       [26]  27  VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS:  Vendor, Cisco       [26]  26  VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS:  Class               [25]  7   6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 5559000000, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 0 0.0.000.0:0000, Accounting-Request,
len 775
00:03:13: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:13: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:13: RADIUS:  User-Name           [1]   8   "123456"
00:03:13: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:03:13: RADIUS:  Calling-Station-Id  [31]  12  "5559000000"
```

```
00:03:13: RADIUS:  Acct-Status-Type    [40]  6   Stop
00:03:13: RADIUS:  Class               [25]  7   6C6F63616C
00:03:13: RADIUS:  Undebuggable        [45]  6   00000001
00:03:13: RADIUS:  Service-Type        [6]   6   Login
00:03:13: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS:  Vendor, Cisco       [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  59  VT=28 TL=53
h323-connect-time=*16:02:48.946 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  62  VT=29 TL=56in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  23  VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  21  VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-paks-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS:  Delay-Time          [41]  6   0
00:03:13: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
h323-disconnect-time=*16:03:11.306 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS:  Vendor, Cisco       [26]  28  VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS:  Acct-Session-Id     [44]  10  "00000000"
00:03:13: RADIUS:  Acct-Input-Octets   [42]  6   0
00:03:13: RADIUS:  Acct-Output-Octets  [43]  6   88000
00:03:13: RADIUS:  Acct-Input-Packets  [47]  6   0
00:03:13: RADIUS:  Acct-Output-Packets [48]  6   550
00:03:13: RADIUS:  Acct-Session-Time   [46]  6   22
00:03:13: RADIUS:  Vendor, Cisco       [26]  30  VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS:  Vendor, Cisco       [26]  35  VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-bytes-
```

The following is sample output from the **debug radius brief** command:

Example:

```
Router# debug radius brief
Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 0 00.0.0.0:0000, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:00 is now connected to 5559000000
00:05:26: RADIUS: Retransmit id 6
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No valid server found. Trying any viable server
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No response for id 7
00:05:31: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 0 0.0.000.0:0000, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 5559000000, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
```

The following example shows **debug radius hex** command output:

Example:

```
Router# debug radius hex
Radius protocol debugging is on
Radius packet hex dump debugging is on
Router#
17:26:52: RADIUS: ustruct sharecount=3
17:26:52: Radius: radius_port_info() success=0 radius_nas_port=1
17:26:52: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Accounting-Request,
len 361
17:26:52:         Attribute 4 6 01081D03
17:26:52:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:26:52:         Attribute 61 6 00000000
17:26:52:         Attribute 1 12 34303835323734323036
17:26:52:         Attribute 30 7 3532393831
17:26:52:         Attribute 31 12 34303835323734323036
17:26:52:         Attribute 40 6 00000001
17:26:52:         Attribute 6 6 00000001
17:26:52:         Attribute 26 27 000000092115683332332D67772D69643D353330305F34332E
17:26:52:         Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
203020334245373142 38
17:26:52:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:26:52:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:26:52:         Attribute 26 56
000000091932683332332D73657475702D74696D653D2A30393A32363A35322E383830205053542053617420536174204A
616E20312032303030
17:26:52:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
:26:52:         Attribute 44 10 3030303030303035
17:26:52:         Attribute 41 6 00000000
17:26:52: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 0000000000
17:26:52: RADIUS: Received from id 10 10.0.0.1:1824, Accounting-response, len 20
17:27:01: RADIUS: ustruct sharecount=3
17:27:01: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:01: RADIUS: Initial Transmit ISDN 0:D:23 id 11 10.0.0.0:1823, Access-Request, len
173
17:27:01:         Attribute 4 6 01081D03
17:27:01:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:01:         Attribute 61 6 00000000
17:27:01:         Attribute 1 8 313233343536
17:27:01:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:01:         Attribute 31 12 34303835323734323036
17:27:01:         Attribute 2 18 C980D8D0E9A061B3D783C61AA6F27214
17:27:01:         Attribute 26 36
00000009011E683332332D6976722D6F75743D7472616E73616374696F6E49443A33
17:27:01: RADIUS: Received from id 11 0.0.000.0:0000, Access-Accept, len 115
17:27:01:         Attribute 6 6 00000001
17:27:01:         Attribute 26 29 000000096517683332332D6372656469742D616D6F756E743D3435
17:27:01:         Attribute 26 27 000000096615683332332D6372656469742D74696D653D3333
17:27:01:         Attribute 26 26 000000096714683332332D72657475726E2D636F64653D30
17:27:01:         Attribute 25 7 6C6F63616C
17:27:01: RADIUS: saved authorization data for user 61AA0698 at 6215087C
17:27:09: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 5559999999, call
lasted 17 seconds
17:27:09: RADIUS: ustruct sharecount=2
17:27:09: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:09: RADIUS: Sent class "local" at 621508E8 from user 61AA0698
17:27:09: RADIUS: Initial Transmit ISDN 0:D:23 id 12 0.0.000.0:0000, Accounting-Request,
len 776
```

```
17:27:09:         Attribute 4 6 01081D03
17:27:09:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:09:         Attribute 61 6 00000000
17:27:09:         Attribute 1 8 313233343536
17:27:09:         Attribute 30 7 3532393831
17:27:09:         Attribute 31 12 34303835323734323036
17:27:09:         Attribute 40 6 00000002
17:27:09:         Attribute 25 7 6C6F63616C
17:27:09:         Attribute 45 6 00000001
17:27:09:         Attribute 6 6 00000001
17:27:09:         Attribute 26 27 000000092115683332332D67772D69643D353330305F34332E
17:27:09:         Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
20302033424537314238
17:27:09:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:27:09:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:27:09:         Attribute 26 56
000000091932683332332D73657475702D74696D653D2A30393A32363A35322E3838302050535420536174204A
616E20312032303030
17:27:09:         Attribute 26 58
000000091C34683332332D636F6E6E6563742D74696D653D2A30393A32363A35322E3930372050535420536174
204A616E20312032303030
17:27:09:         Attribute 26 61
000000091D37683332332D646973636F6E6E6563742D74696D653D2A30393A32373A31302E3133372050535420
536174204A616E20312032303030
17:27:09:         Attribute 26 32
000000091E1A683332332D646973636F6E6E6563742D63617573653D3130
17:27:09:         Attribute 26 28 000000091F16683332332D766F6963652D7175616C6974793D30
17:27:09:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:09:         Attribute 44 10 3030303030303035
17:27:09:         Attribute 42 6 00000000
17:27:09:         Attribute 43 6 00012CA0
17:27:09:         Attribute 47 6 00000000
17:27:09:         Attribute 48 6 000001E1
17:27:09:         Attribute 46 6 00000011
17:27:09:         Attribute 26 30 0000000901187375627363726962657 23D526567756C61724C696E65
17:27:09:         Attribute 26 35
00000009011D683332332D6976722D6F75743D5461726966663A556E6B6E6F776E
17:27:09:         Attribute 26 22 0000000901107072652D62797465732D696E3D30
17:27:09:         Attribute 26 23 00000009011107265 2D62797465732D6F75743D30
17:27:09:         Attribute 26 21 00000009010F7072652D70616B732D696E3D30
17:27:09:         Attribute 26 22 0000000901107072652D70616B732D6F75743D30
17:27:09:         Attribute 26 22 0000000901106E61732D72782D73706565643D30
17:27:09:         Attribute 26 22 0000000901106E61732D74782D73706565643D30
17:27:09:         Attribute 41 6 00000000
17:27:09: RADIUS: Received from id 12 10.0.0.1:1824, Accounting-response, len 20
```

Configuration Examples for PPPoE Service Selection

Example PPPoE Service Selection with ATM QoS and Tunneling Services

In the following example, three services are configured: gold-isp-A, silver-isp-A, and isp-xyz. The gold and silver services are forwarded onto the same tunnel, but the ATM PVCs between the LAC and DSLAM is set

up with different QoS parameters depending on the level of service chosen. The isp-xyz service offers users access to the services of the xyz Internet service provider.

In this example, the subscriber profile is configured locally on the PPPoE server.

RADIUS Service Profile Configuration

```
gold-isp-A  Password = "cisco", User-Service-type = Outbound-User
        Tunnel-Assignment-Id = nrp1-3,
        Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
        Cisco-Avpair = "atm:peak-cell-rate =2500",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =400"
silver-isp-A  Password = "cisco",  User-Service-type = Outbound-User
        Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
        Cisco:Cisco-Avpair = "atm:peak-cell-rate =1500",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =200"
isp-xyz  Password = "cisco", User-Service-type = Outbound-User
        Cisco-Avpair = "vpdn:tunnel-id=aol",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.5",
        Cisco:Cisco-Avpair = "atm:peak-cell-rate =1000",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =150"
```

PPPoE Server Configuration

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default local
!
!subscriber authorization enable
! Configure the subscriber profile
policy-map type service listA
 pppoe service gold-isp-A
 pppoe service silver-isp-A
 pppoe service isp-xyz
!
! Configure the PPPoE profile
bba-group pppoe group-A
 virtual-template 1
 sessions per-vc limit 5
 service profile listA
! Attach the PPPoE profile to a PVC
interface atm0/0.0
 pvc 2/200
  protocol PPPoE group group-A
!
```

Example PPPoE Service Selection with Tunneling Services

In the following example, PPPoE service selection is used to provide tunneling services only. In this example, the subscriber profile is configured on the RADIUS server.

RADIUS Service Profile Configuration

```
tunnel-to-cust1 Password = "cisco", User-Service-type = Outbound-User
   Tunnel-Assignment-Id = nrp1-3,
   Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
tunnel-to-cust2 Password = "cisco", User-Service-type = Outbound-User
   Cisco-Avpair = "vpdn:tunnel-id=xyz",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.5",

tunnel-to-cust3 Password = "cisco", User-Service-type = Outbound-User
   Cisco-Avpair = "vpdn:tunnel-id=aol",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.6",
```

RADIUS Subscriber Profile Configuration

```
customer-tunnels Password = "cisco", User-Service-type = Outbound-User
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust1",
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust2",
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust3"
```

PPPoE Server Configuration

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default group radius
!
! Configure the PPPoE profile
bba-group pppoe group-A
 virtual-template 1
 sessions per-vc  5
 service profile customer-tunnels
!
! Attach the PPPoE profile to PVCs
interface atm0/1/0.10
 pvc 2/200
  protocol PPPoE group pppoe-group-A
!
interface atm0/1/0.10
 pvc 3/300
  protocol PPPoE group pppoe-group-A
```

Where to Go Next

- If you want to establish PPPoE sessions limits for sessions on a specific permanent virtual circuit or VLAN configured on an L2TP access concentrator, refer to the "Establishing PPPoE Session Limits per NAS Port" module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to an LNS or tunnel switch, refer to the "Enabling PPPoE Relay Discovery and Service Selection Functionality" module.

- If you want to configure the transfer upstream of the Point-to-Point Protocol over X (family of encapsulating communications protocols implementing PPP)(PPPoX) session speed value, refer to the "Configuring Upstream Connections Speed Transfer" module.
- If you want to use the Simple Network Management Protocol (SNMP) to monitor PPPoE sessions, refer to the "Monitoring PPPoE Sessions with SNMP" module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, refer to the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, refer to the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

Related Documents

Related Topic	Document Title
RADIUS attributes and configuration	*Cisco IOS XE Security Configuration Guide*, Release 2
Tunneling configuration	*Cisco IOS XE Dial Technologies Configuration Guide* , Release 2
Broadband access aggregation concepts, preparing for broadband access aggregation, and configuring PPPoE sessions	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*, Release 2
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS XE Broadband Access Aggregation and DSL Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature. Support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE), February 1999

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

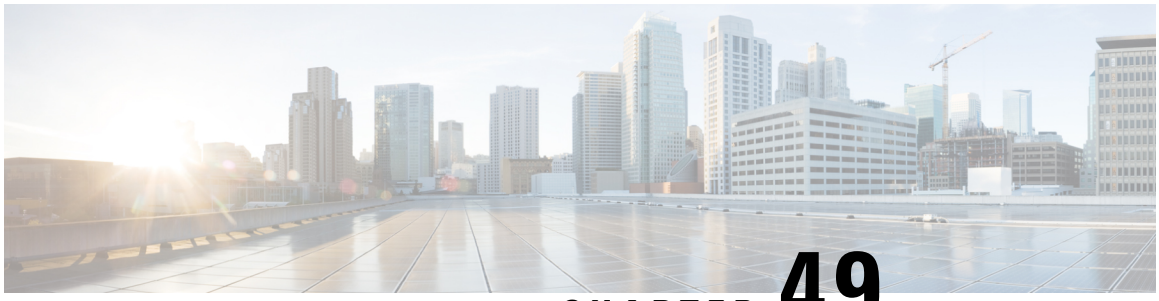
Feature Information for PPPoE Service Selection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 59: Feature Information for PPPoE Service Selection

Feature Name	Releases	Feature Configuration Information
PPPoE Service Selection	Cisco IOS XE Release 2.1	The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. You choose one of the services offered, and the service is provided when the PPPoE session becomes active. The following commands were introduced or modified: **service profile**, **pppoe service**, **virtual-template**.



CHAPTER 49

Disabling AC-name and AC-cookie Tags from PPPoE PADS

The AC-name and AC-cookie Tags from PPP over Ethernet (PPPoE) Active Directory Session (PADS) feature prevents a device from sending the access concentrator (AC) information in the PADS packet.

Restrictions for Disabling AC-name and AC-cookie Tags from PPPoE PADS

- The AC-name and AC-cookie Tags from PPPoE PADS feature is available only on ASR and UNIX platforms.
- The AC-name and AC-cookie Tags from PPPoE PADS feature is supported only if the PPPoE Server functionality is supported.

Information About Disabling AC-name and AC-cookie Tags from PPPoE PADS

In the Broadband Access (BBA) environment, PPPoE Active Discovery Offer (PADO) sent from the Broadband Remote Access Server (BRAS) includes the AC-cookie tags (0x0104) and the AC-name tag (0x0102) along with a service-name tag identical to the one in the PPPoE Active Directory Initiation (PADI) and any number of other service-name tags indicating other services that access concentrator (AC) offers.

The AC-name is a string that uniquely identifies the particular AC. The AC-cookie tags are used by the AC to protect the denial-of-service (DoS) attacks.

The PPPoE Active Directory Request (PADR) from the Customer Premise Equipment (CPE) host also includes AC-name and AC-cookie tags received in PADO. BRAS repeats the AC information in the PPPoE Active Discovery Session-Confirmation (PADS) packet sent in response to PADR received from client (CPE).

When BRAS generates a unique session identifier for the PPPoE session, the AC-name and AC-cookie tags need not be sent in the PADS. This feature prevents sending the AC information in the device.

How to Disable AC-name and AC-cookie Tags from PPPoE PADS

Disabling AC-name and AC-cookie Tags from PPPoE PADS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pppoe pads disable-ac-info**
4. **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	**pppoe pads disable-ac-info** **Example:** `Device(config)# pppoe pads disable-ac-info`	Defines a PPP over Ethernet (PPPoE) profile, and prevents the device from sending the AC-name and AC-cookie tags in the PADS packet.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Disabling AC-name and AC-cookie Tags from PPPoE PADS

You can verify the Disabling AC-name and AC-cookie Tags from PPPoE PADS feature by enabling the **debug pppoe tag** command.

```
Device> enable
Device# debug pppoe tag
*Sep  6 07:46:25.352: PPPoE 0: I PADI  R:aabb.cc00.6401 L:ffff.ffff.ffff Et1/0
*Sep  6 07:46:25.352:  Service tag: NULL Tag
*Sep  6 07:46:25.352: PPPoE 0: O PADO, R:aabb.cc00.6501 L:aabb.cc00.6401 Et1/0
*Sep  6 07:46:25.352:  Service tag: NULL Tag
*Sep  6 07:46:25.353: PPPoE 0: I PADR  R:aabb.cc00.6401 L:aabb.cc00.6501 Et1/0
*Sep  6 07:46:25.353:  Service tag: NULL Tag
*Sep  6 07:46:25.353: PPPoE : encap string prepared
*Sep  6 07:46:25.353: [2]PPPoE 2: Access IE handle allocated
*Sep  6 07:46:25.353: [2]PPPoE 2: AAA get retrieved attrs
*Sep  6 07:46:25.353: [2]PPPoE 2: AAA get nas port details
*Sep  6 07:46:25.353: [2]PPPoE 2: AAA get dynamic attrs
*Sep  6 07:46:25.353: [2]PPPoE 2: AAA unique ID D allocated
*Sep  6 07:46:25.353: [2]PPPoE 2: No AAA accounting method list
*Sep  6 07:46:25.353: [2]PPPoE 2: Service request sent to SSS
*Sep  6 07:46:25.354: [2]PPPoE 2: Created, Service: None R:aabb.cc00.6501 L:aabb.cc00.6401
 Et1/0
*Sep  6 07:46:25.354: [2]PPPoE 2: State NAS_PORT_POLICY_INQUIRY    Event SSS MORE KEYS
*Sep  6 07:46:25.354: [2]PPPoE 2: data path set to PPP
*Sep  6 07:46:25.354: [2]PPPoE 2: Segment (SSS class): PROVISION
*Sep  6 07:46:25.354: [2]PPPoE 2: State PROVISION_PPP    Event SSM PROVISIONED
*Sep  6 07:46:25.354: [2]PPPoE 2: Disable AC info from PADS
*Sep  6 07:46:25.354: [2]PPPoE 2: O PADS  R:aabb.cc00.6401 L:aabb.cc00.6501 Et1/0
```

Configuration Example for Disabling AC-name and AC-cookie Tags from PPPoE PADS

Example: Disabling AC-name and AC-cookie Tags from PPPoE PADS

```
Device> enable
Device# configure terminal
Device(config)# pppoe pads disable-ac-info
Device(config)# end
```

Additional References for Disabling AC-name and AC-cookie Tags from PPPoE PADS

Related Documents

Related Topic	Document Title

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

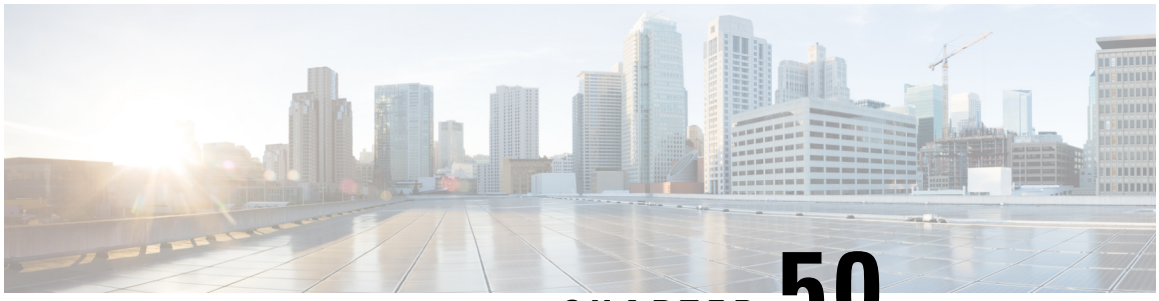
Feature Information for Disabling AC-name and AC-cookie Tags from PPPoE PADS

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 60: Feature Information for Disabling AC-name and AC-cookie Tags from PPPoE PADS

Feature Name	Releases	Feature Information
AC-name and AC-cookie knob for PPPoE PADS	Cisco IOS XE Release 3.12S	This feature prevents a device from sending access concentrator information in the PADS packet. The following commands were introduced or modified: **pppoe pads disable-ac-info**.



CHAPTER 50

Broadband Smart Licensing

The Broadband Smart Licensing feature supports broadband Lite sessions during the deployment of ASR1000 Aggregation Services Routers.

Information About Broadband Smart Licensing

In traditional licenses, you have a limited view on license that you own. It requires manual registration to product activation key, where each user has to visit website to register licenses for each product individually.

In smart licenses, customers and partners have a complete view on the licenses. To view these licenses, you need log in to software.cisco.com. After registering to the smart account, the product registration allows easy activation.

Broadband licensing feature is all about moving from traditional licensing to broadband smart licensing where you purchase licenses only for the number of broadband sessions that you brought up during the deployment of Cisco ASR 1000 Series Aggregation Services Routers. For information about smart licensing, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.

Managing Smart Licenses

The following procedure shows how to manage smart licenses:

1. Buy licenses from the Cisco commerce workspace and assign to a customer smart account.
2. Log in to sofware.cisco.com and view available license pool in Cisco Smart Software Manager(CSSM).
3. Generate the token for the ASR1K device which we are going to use and register the device in CSSM.
4. Configure the smart license in ASR1K device.

After you perform this procedure, you are ready to consume the broadband licenses on a registered device.

Restrictions for Broadband Smart Licensing

- The Broadband Smart Licensing feature is supported only on AR1K running Polaris 16.5 release and above.
- The feature does not support boradband Lite sessions.
- The stand-by RP does not have an account.
- Only broadband smart licenses that are multiples of two can be requested, 1 license = 2 thousand sessions.

How to Configure Broadband Smart Licensing

Configuring the Subscriber License

To configure broadband smart licensing, configure the **subscriber license** command before starting a broadband session.

Before you begin

Do the following:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber license**
4. **exit**

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	**subscriber license** **Example:**	Configures the subscriber license.

	Command or Action	Purpose

	`Device(config)# subscriber license`	**Note**
		• The following configurations are essential to establish a connection between the ASR1000 and the licensing server.
		  • License Smart Enable
		  • Call Home
		  • Device Registration
		• If the **subscriber license** command is configured before bringing up a broadband session, irrespective of any earlier broadband license request failure, the range of the license to be requested must be between 2 – 128K (range of subscriber license). When the session count exceeds the procured broadband license count by 100, a request is sent for a new license.
		Ensure that there is no failure of license procurement in the last 24 hours.
		• Use the **no subscriber license** command to release all the procured licenses and reset the value to default, that is, zero licenses. You can use this command only when there are no active sessions.

Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Clearing the Subscriber License

SUMMARY STEPS

1. **clear subscriber license**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear subscriber license**	Releases the licenses. **Note** The **clear** command releases the licenses based on the active sessions and procured licenses.

Verifying Broadband Smart Licensing

SUMMARY STEPS

1. **Debug subscriber license**

DETAILED STEPS

Debug subscriber license

Configuration Examples for Broadband Smart Licensing

Example: Configuring Smart License

The following example shows how to configure smart license in Cisco ASR 1000 Series Aggregation Services Routers.

```
UUT#config
UUT(config)#service internal
UUT(config)#license smart transport smart
UUT(config)#license smart url https://smartreceiver-stage.cisco.com/licservice/license
UUT(config)#license smart url smart  https://smartreceiver.cisco.com/licservice/license
```

Example: Configuring License Boot Level

For UniversalK9 image, there are three types of License Boot level:

- adventerprise (AES)
- advipservices (AIS)
- ipbase (IPB)

When your router is booted with UniversalK9 image, there must be one boot level present on the router.

To activate boot level, run the following commands:

```
UUT#config
UUT(config)#license boot level adventerprise
% use 'write' command to make license boot config take effect on next boot
UUT(config)#write
UUT(config)#end
UUT#
UUT#reload
```

After reloading the chassis, you can see the license in box:

```
UUT#sh license summary
License Usage:
    License                Entitlement Tag              Count Status
```

```
--------------------------------------------------------------------------------
adventerprise           (ASR_1000_AdvEnterprise)          1 IN USE
```

Example: show subscriber license

The **show subscriber license** command tracks the number of procured broadband licenses, the configured value of broadband licenses, current session count on the router, the highest session count reached since the last license request was sent to the server and the time at which it was procured.

The following is sample output of the **show subscriber license** command

```
Device# show subscriber license
Broadband Smart License Compliance              : In Compliance

Total Number of Broadband Licenses Procured     : 0

Broadband Licenses Configured                   : 0

Current Broadband Session Count                 : 0

Time of Last License Procurement                : No License Procured

Sessions Peak Count Since Last Procurement      : 0
```

Disable Subscriber License

Use the **no subscriber license** command to release all the procured licenses and reset the value to default, that is, zero licenses.

```
Device# no subscriber license
```

Example: Show license summary

To display the license summary, use the **show license summary** command.

```
Device# show license summary
License Usage:
  License                Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  broadband              (ASR_1000_BroadBand_2K)          16 IN USE
  adventerprise          (ASR_1000_AdvEnterprise)          1 IN USE
UUT#
UUT#sh subscriber license
Broadband Smart License Compliance              : In Compliance
Total Number of Broadband Licenses Procured     : 2000
Broadband Licenses Configured                   : 0
Current Broadband Session Count                 : 32000
Time of Last License Procurement                : Mon Sep 27 11:32:07 2021
Sessions Peak Count Since Last Procurement      : 32000
```

Example: Clear subscriber license

```
Device# clear subscriber license

*Jul 10 10:24:27.217: %SSSMGR-5-BB_LICENSE_REQUEST_SENT: Broadband license request sent for
 0 license with configured license count 0

*Jul 10 10:24:27.217: %SSSMGR-5-BB_LICENSE_RELEASE_SUCCESS: Successfully released all
BroadBand licenses


Sessions: ISG session, except for the lite session
```

Additional References for Broadband Smart Licensing

Related Documents

Related Topic	Document Title
Smart Licensing Using Policy for Cisco Enterprise Routing Platforms	https://www.cisco.com/c/en/us/td/docs/routers/sl_using_policy/b-sl-using-policy.html

MIBs

MIB	MIBs Link
• CISCO-SMB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Broadband Smart Licensing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

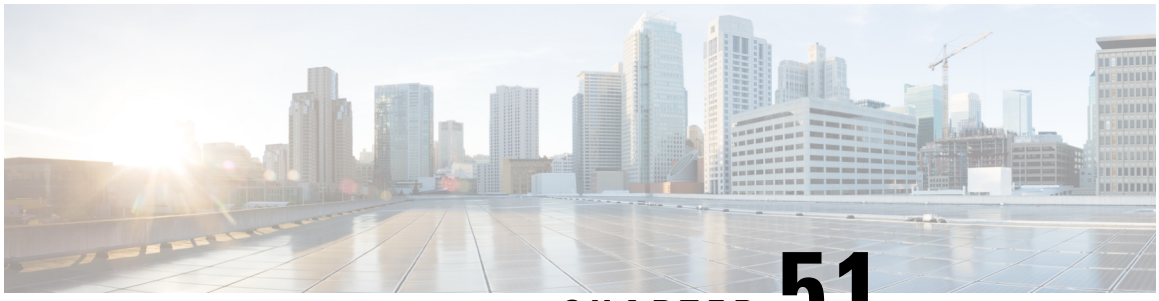
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 61: Feature Information for Broadband Smart Licensing

Feature Name	Releases	Feature Information
Broadband Smart Licensing	Cisco IOS XE Everest 16.6.1	The Broadband Smart Licensing feature enables to purchase licenses for any number of broadband sessions that are active during the deployment of Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **subscriber license**, **show subscriber license**

PART III

Carrier Ethernet



CHAPTER 51

Using Ethernet Operations Administration and Maintenance

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the Open Systems Interconnection (OSI) model. The OAM features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions.

The advent of Ethernet as a MAN and WAN technology has emphasized the necessity for integrated management for larger deployments. For Ethernet to extend into public MANs and WANs, it must be equipped with a new set of requirements on Ethernet's traditional operations, which had been centered on enterprise networks only. The expansion of Ethernet technology into the domain of service providers, where networks are substantially larger and more complex than enterprise networks and the user-base is wider, makes operational management of link uptime crucial.

Information About Using Ethernet Operations Administration and Maintenance

Ethernet OAM

Ethernet OAM is a protocol for installing, monitoring, and troubleshooting metro Ethernet networks and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the OSI model. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. A system-wide implementation is not required; OAM can be deployed for part of a system; that is, on particular interfaces.

Normal link operation does not require Ethernet OAM. OAM frames, called OAM protocol data units (PDUs), use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network.

Ethernet OAM is a relatively slow protocol with modest bandwidth requirements. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on normal operations is negligible. However, when link monitoring is enabled, the CPU must poll error counters frequently. In this case, the required CPU cycles will be proportional to the number of interfaces that have to be polled.

Two major components, the OAM client and the OAM sublayer, make up Ethernet OAM. The following two sections describe these components.

OAM Client

The OAM client is responsible for establishing and managing Ethernet OAM on a link. The OAM client also enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality on the link based on local and remote state as well as configuration settings. Beyond the discovery phase (at steady state), the OAM client is responsible for managing the rules of response to OAM PDUs and managing the OAM remote loopback mode.

OAM Sublayer

The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces: one facing toward the superior sublayers, which include the MAC client (or link aggregation), and the other interface facing toward the subordinate MAC control sublayer. The OAM sublayer provides a dedicated interface for passing OAM control information and OAM PDUs to and from a client.

The OAM sublayer is made up of three components: control block, multiplexer, and packet parser (p-parser). Each component is described in the following sections.

Control Block

The control block provides the interface between the OAM client and other blocks internal to the OAM sublayer. The control block incorporates the discovery process, which detects the existence and capabilities of remote OAM peers. It also includes the transmit process that governs the transmission of OAM PDUs to the multiplexer and a set of rules that govern the receipt of OAM PDUs from the p-parser.

Multiplexer

The multiplexer manages frames generated (or relayed) from the MAC client, control block, and p-parser. The multiplexer passes through frames generated by the MAC client untouched. It passes OAM PDUs generated by the control block to the subordinate sublayer; for example, the MAC sublayer. Similarly, the multiplexer passes loopback frames from the p-parser to the same subordinate sublayer when the interface is in OAM remote loopback mode.

P-Parser

The p-parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and then dispatches each class to the appropriate entity. OAM PDUs are sent to the control block. MAC client frames are passed to the superior sublayer. Loopback frames are dispatched to the multiplexer.

Benefits of Ethernet OAM

Ethernet OAM provides the following benefits:

- Competitive advantage for service providers.

- Standardized mechanism to monitor the health of a link and perform diagnostics.

Note REP traps are prioritized when both Ethernet OAM and REP traps are configured on the same port. If you want to view Ethernet OAM logs, then you must disable REP configurations.

Cisco Implementation of Ethernet OAM

The Cisco implementation of Ethernet OAM consists of the Ethernet OAM shim and the Ethernet OAM module.

The Ethernet OAM shim is a thin layer that connects the Ethernet OAM module and the platform code. It is implemented in the platform code (driver). The shim also communicates port state and error conditions to the Ethernet OAM module via control signals.

The Ethernet OAM module, implemented within the control plane, handles the OAM client as well as control block functionality of the OAM sublayer. This module interacts with the CLI and Simple Network Management Protocol (SNMP)/programmatic interface via control signals. In addition, this module interacts with the Ethernet OAM shim through OAM PDU flows.

OAM Features

The OAM features as defined by IEEE 802.3ah, *Ethernet in the First Mile*, are discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions.

Discovery

Discovery is the first phase of Ethernet OAM and it identifies the devices in the network and their OAM capabilities. Discovery uses information OAM PDUs. During the discovery phase, the following information is advertised within periodic information OAM PDUs:

- OAM mode—Conveyed to the remote OAM entity. The mode can be either active or passive and can be used to determine device functionality.
- OAM configuration (capabilities)—Advertises the capabilities of the local OAM entity. With this information a peer can determine what functions are supported and accessible; for example, loopback capability.
- OAM PDU configuration—Includes the maximum OAM PDU size for receipt and delivery. This information along with the rate limiting of 10 frames per second can be used to limit the bandwidth allocated to OAM traffic.
- Platform identity—A combination of an organization unique identifier (OUI) and 32-bits of vendor-specific information. OUI allocation, controlled by the IEEE, is typically the first three bytes of a MAC address.

Discovery includes an optional phase in which the local station can accept or reject the configuration of the peer OAM entity. For example, a node may require that its partner support loopback capability to be accepted into the management network. These policy decisions may be implemented as vendor-specific extensions.

Link Monitoring

Link monitoring in Ethernet OAM detects and indicates link faults under a variety of conditions. Link monitoring uses the event notification OAM PDU and sends events to the remote OAM entity when there are problems detected on the link. The error events include the following:

- Error Symbol Period (error symbols per second)—The number of symbol errors that occurred during a specified period exceeded a threshold. These errors are coding symbol errors.
- Error Frame (error frames per second)—The number of frame errors detected during a specified period exceeded a threshold.
- Error Frame Period (error frames per *n* frames)—The number of frame errors within the last n frames has exceeded a threshold.
- Error Frame Seconds Summary (error seconds per *m* seconds)—The number of error seconds (1-second intervals with at least one frame error) within the last m seconds has exceeded a threshold.

Since IEEE 802.3ah OAM does not provide a guaranteed delivery of any OAM PDU, the event notification OAM PDU may be sent multiple times to reduce the probability of a lost notification. A sequence number is used to recognize duplicate events.

Remote Failure Indication

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. The following failure conditions can be communicated:

- Link Fault—Loss of signal is detected by the receiver; for instance, the peer's laser is malfunctioning. A link fault is sent once per second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.
- Dying Gasp—An unrecoverable condition has occurred; for example, when an interface is shut down. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.

  For more information on Dying Gasp, see the Dying Gasp Support for Loss of Power Supply Through SNMP, Syslog and Ethernet OAM chapter in the Cisco NCS 520 Series Router Configuration Guide.
- Critical Event—An unspecified critical event has occurred. This type of event is vendor specific. A critical event may be sent immediately and continuously.

Remote Loopback

An OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

The loopback command is acknowledged by responding with an information OAM PDU with the loopback state indicated in the state field. This acknowledgement allows an administrator, for example, to estimate if a network segment can satisfy a service-level agreement. Acknowledgement makes it possible to test delay, jitter, and throughput.

When an interface is set to the remote loopback mode the interface no longer participates in any other Layer 2 or Layer 3 protocols; for example Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). The

reason is that when two connected ports are in a loopback session, no frames other than the OAM PDUs are sent to the CPU for software processing. The non-OAM PDU frames are either looped back at the MAC level or discarded at the MAC level.

From a user's perspective, an interface in loopback mode is in a link-up state.

Cisco Vendor-Specific Extensions

Ethernet OAM allows vendors to extend the protocol by allowing them to create their own type-length-value (TLV) fields.

OAM Messages

Ethernet OAM messages or OAM PDUs are standard length, untagged Ethernet frames within the normal frame length bounds of 64 to 1518 bytes. The maximum OAM PDU frame size exchanged between two peers is negotiated during the discovery phase.

OAM PDUs always have the destination address of slow protocols (0180.c200.0002) and an Ethertype of 8809. OAM PDUs do not go beyond a single hop and have a hard-set maximum transmission rate of 10 OAM PDUs per second. Some OAM PDU types may be transmitted multiple times to increase the likelihood that they will be successfully received on a deteriorating link.

Four types of OAM messages are supported:

- Information OAM PDU--A variable-length OAM PDU that is used for discovery. This OAM PDU includes local, remote, and organization-specific information.
- Event notification OAM PDU--A variable-length OAM PDU that is used for link monitoring. This type of OAM PDU may be transmitted multiple times to increase the chance of a successful receipt; for example, in the case of high-bit errors. Event notification OAM PDUs also may include a time stamp when generated.
- Loopback control OAM PDU--An OAM PDU fixed at 64 bytes in length that is used to enable or disable the remote loopback command.
- Vendor-specific OAM PDU--A variable-length OAM PDU that allows the addition of vendor-specific extensions to OAM.

IEEE 802.3ah Link Fault RFI Support

The IEEE 802.3ah Link Fault RFI Support feature provides a per-port configurable option that moves a port into a blocking state when an OAM PDU control request packet is received with the Link Fault Status flag set. In the blocking state, the port can continue to receive OAM PDUs, detect remote link status, and automatically recover when the remote link becomes operational. When an OAM PDU is received with the Link Fault Status flag set to zero or FALSE, the port is enabled and all VLANs configured on the port are set to "forwarding."

Note If you configure the Ethernet OAM timeout period to be the minimum allowable value of 2 seconds, the Ethernet OAM session may be dropped briefly when the port transitions from blocked to unblocked. This action will not occur by default; the default timeout value is 5 seconds.

Before the release of the IEEE 802.3ah Link Fault RFI Support feature, when an OAM PDU control request packet was received with the Link Fault Status flag set, one of three actions was taken:

- A warning message was displayed or logged, and the port remained operational.
- The Link Fault Status flag was ignored.

Ethernet Connectivity Fault Management

Ethernet connectivity fault management (CFM) is an end-to-end per-service-instance Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End to end can be provider edge (PE) to PE or customer edge (CE) to CE. Per service instance means per VLAN.

For more information about Ethernet CFM, see Ethernet Connectivity Fault Management .

High Availability Features Supported by 802.3ah

In access and service provider networks using Ethernet technology, High Availability (HA) is a requirement, especially on Ethernet OAM components that manage Ethernet virtual circuit (EVC) connectivity. End-to-end connectivity status information is critical and must be maintained on a hot standby Route Switch Processor (RSP) (a standby RSP that has the same software image as the active RSP and supports synchronization of line card, protocol, and application state information between RSPs for supported features and protocols). End-to-end connectivity status is maintained on the CE, PE, and access aggregation PE (uPE) network nodes based on information received by protocols such as CFM and 802.3ah. This status information is used to either stop traffic or switch to backup paths when an EVC is down. Metro Ethernet clients (for example, CFM and 802.3ah) maintain configuration data and dynamic data, which is learned through protocols. Every transaction involves either accessing or updating data among the various databases. If the databases are synchronized across active and standby modules, the RSPs are transparent to clients.

Cisco infrastructure provides various component application program interfaces (APIs) for clients that are helpful in maintaining a hot standby RSP. Metro Ethernet HA clients (such as, HA/ISSU, CFM HA/ISSU, 802.3ah HA/ISSU) interact with these components, update the databases, and trigger necessary events to other components.

Benefits of 802.3ah HA

- Elimination of network downtime for Cisco software image upgrades, resulting in higher availability
- Elimination of resource scheduling challenges associated with planned outages and late night maintenance windows
- Accelerated deployment of new services and applications and faster implementation of new features, hardware, and fixes due to the elimination of network downtime during upgrades
- Reduced operating costs due to outages while delivering higher service levels due to the elimination of network downtime during upgrades

NSF SSO Support in 802.3ah OAM

The redundancy configurations Stateful Switchover (SSO) and Nonstop Forwarding (NSF) are both supported in Ethernet OAM and are automatically enabled. A switchover from an active to a standby Route Switch Processor (RSP) occurs when the active RSP fails, is removed from the networking device, or is manually

taken down for maintenance. NSF interoperates with the SSO feature to minimize network downtime following a switchover. The primary function of Cisco NSF is to continue forwarding IP packets following an RSP switchover.

For detailed information about the SSO feature, see the "Configuring Stateful Switchover" module of the *High Availability Configuration Guide*. For detailed information about the NSF feature, see the "Configuring Cisco Nonstop Forwarding" module of the *High Availability Configuration Guide.*

ISSU Support in 802.3ah OAM

Cisco In-Service Software Upgrades (ISSUs) allow you to perform a Cisco software upgrade or downgrade without disrupting packet flow. ISSU is automatically enabled in 802.3ah. OAM performs a bulk update and a runtime update of the continuity check database to the standby Route Switch Processor (RSP), including adding, deleting, or updating a row. This checkpoint data requires ISSU capability to transform messages from one release to another. All the components that perform active RSP to standby RSP updates using messages require ISSU support.

ISSU lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. For detailed information about ISSU, see the "Performing an In Service Software Upgrade" module of the *High Availability Configuration Guide*.

How to Set Up and Configure Ethernet Operations Administration and Maintenance

Enabling Ethernet OAM on an Interface

Ethernet OAM is by default disabled on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]
5. **exit**

DETAILED STEPS

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** *type number*

Example:

Specifies an interface and enters interface configuration mode.

Step 4 **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]

Example:

```
Device(config-if)# ethernet oam
```

Enables Ethernet OAM.

Step 5 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Disabling and Enabling a Link Monitoring Session

Link monitoring is enabled by default when you enable Ethernet OAM. Perform these tasks to disable and enable link monitoring sessions:

Disabling a Link Monitoring Session

Perform this task to disable a link monitoring session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]
5. **no ethernet oam link-monitor supported**
6. **exit**

DETAILED STEPS

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** *type number*

Example:

Specifies an interface and enters interface configuration mode.

Step 4 **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]

Example:

```
Device(config-if)# ethernet oam
```

Enables Ethernet OAM.

Step 5 **no ethernet oam link-monitor supported**

Example:

```
Device(config-if)# no ethernet oam link-monitor supported
```

Disables link monitoring on the interface.

Step 6 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Enabling a Link Monitoring Session

Perform this task to reenable a link monitoring session after it was previously disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam link-monitor supported**
5. **exit**

DETAILED STEPS

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** *type number*

Example:

Specifies an interface and enters interface configuration mode.

Step 4 **ethernet oam link-monitor supported**

Example:

```
Device(config-if)# ethernet oam link-monitor supported
```

Enables link monitoring on the interface.

Step 5 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Stopping and Starting Link Monitoring Operations

Link monitoring operations start automatically when Ethernet OAM is enabled on an interface. When link monitoring operations are stopped, the interface does not actively send or receive event notification OAM PDUs. The tasks in this section describe how to stop and start link monitoring operations.

Stopping Link Monitoring Operations

Perform this task to stop link monitoring operations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]
5. **no ethernet oam link-monitor on**
6. **exit**

DETAILED STEPS

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** *type number*

Example:

Specifies an interface and enters interface configuration mode.

Step 4 **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]

Example:

```
Device(config-if)# ethernet oam
```

Enables Ethernet OAM.

Step 5 **no ethernet oam link-monitor on**

Example:

```
Device(config-if)# no ethernet oam link-monitor on
```

Stops link monitoring operations.

Step 6 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Starting Link Monitoring Operations

Perform this task to start link monitoring operations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam link-monitor on**
5. **exit**

DETAILED STEPS

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** *type number*

Example:

Specifies an interface and enters interface configuration mode.

Step 4 **ethernet oam link-monitor on**

Example:

```
Device(config-if)# ethernet oam link-monitor on
```

Starts link monitoring operations.

Step 5 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Configuring Link Monitoring Options

Perform this optional task to specify link monitoring options. Steps 4 through 10 can be performed in any sequence.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]
5. **ethernet oam link-monitor frame** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}
6. **ethernet oam link-monitor frame-period** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *frames*}
7. **ethernet oam link-monitor frame-seconds** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}
8. **ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}
9. **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}
10. **ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none** | *high-symbols*} | **low** *low-symbols*} | **window** *symbols*}
11. **exit**

DETAILED STEPS

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** *type number*

Example:

Identifies the interface and enters interface configuration mode.

Step 4 **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]

Example:

```
Device(config-if)# ethernet oam
```

Enables Ethernet OAM.

Step 5 **ethernet oam link-monitor frame** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-if)# ethernet oam link-monitor frame window 399
```

Configures a number for error frames that when reached triggers an action.

Step 6 **ethernet oam link-monitor frame-period** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *frames*}

Example:

```
Device(config-if)# ethernet oam link-monitor frame-period threshold high 599
```

Configures a number of frames to be polled.

Frame period is a user-defined parameter.

Step 7 **ethernet oam link-monitor frame-seconds** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-if)# ethernet oam link-monitor frame-seconds window 699
```

Configures a period of time in which error frames are counted.

Step 8 **ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-if)# ethernet oam link-monitor receive-crc window 99
```

Configures an Ethernet OAM interface to monitor ingress frames with cyclic redundancy check (CRC) errors for a period of time.

Step 9 **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-if)# ethernet oam link-monitor transmit-crc threshold low 199
```

Configures an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time.

Step 10 **ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none** | *high-symbols*} | **low** *low-symbols*} | **window** *symbols*}

Example:

```
Device(config-if)# ethernet oam link-monitor symbol-period threshold high 299
```

Configures a threshold or window for error symbols, in number of symbols.

Step 11 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Example

Configuring Global Ethernet OAM Options Using a Template

Perform this task to create a template to use for configuring a common set of options on multiple Ethernet OAM interfaces. Steps 4 through 10 are optional and can be performed in any sequence. These steps may also be repeated to configure different options.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **template** *template-name*
4. **ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}
5. **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}
6. **ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none** | *high-symbols*} | **low** *low-symbols*} | **window** *symbols*}
7. **ethernet oam link-monitor frame** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}
8. **ethernet oam link-monitor frame-period** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *frames*}
9. **ethernet oam link-monitor frame-seconds** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}
10. **exit**
11. **interface** *type number*
12. **source template** *template-name*
13. **exit**
14. **exit**
15. **show running-config**

DETAILED STEPS

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 **template** *template-name*

Example:

```
Device(config)# template oam-temp
```

Configures a template and enters template configuration mode.

Step 4 **ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-template)# ethernet oam link-monitor receive-crc window 99
```

Configures an Ethernet OAM interface to monitor ingress frames with CRC errors for a period of time.

Step 5 **ethernet oam link-monitor transmit-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-template)# ethernet oam link-monitor transmit-crc threshold low 199
```

Configures an Ethernet OAM interface to monitor egress frames with CRC errors for a period of time.

Step 6 **ethernet oam link-monitor symbol-period** {**threshold** {**high** {**none** | *high-symbols*} | **low** *low-symbols*} | **window** *symbols*}

Example:

```
Device(config-template)# ethernet oam link-monitor symbol-period threshold high 299
```

Configures a threshold or window for error symbols, in number of symbols.

Step 7 **ethernet oam link-monitor frame** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-template)# ethernet oam link-monitor frame window 399
```

Configures a number for error frames that when reached triggers an action.

Step 8 **ethernet oam link-monitor frame-period** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *frames*}

Example:

```
Device(config-template)# ethernet oam link-monitor frame-period threshold high 599
```

Configures a number of frames to be polled.

Frame period is a user-defined parameter.

Step 9 **ethernet oam link-monitor frame-seconds** {**threshold** {**high** {**none** | *high-frames*} | **low** *low-frames*} | **window** *milliseconds*}

Example:

```
Device(config-template)# ethernet oam link-monitor frame-seconds window 699
```

Configures a period of time in which error frames are counted.

Step 10 **exit**

Example:

```
Device(config-template)# exit
```

Returns to global configuration mode.

Step 11 **interface** *type number*

Example:

Identifies the interface on which to use the template and enters interface configuration mode.

Step 12 **source template** *template-name*

Example:

```
Device(config-if)# source template oam-temp
```

Applies to the interface the options configured in the template.

Step 13 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Step 14 **exit**

Example:

```
Device(config)# exit
```

Returns to privileged EXEC mode.

Step 15 **show running-config**

Example:

```
Device# show running-config
```

Displays the updated running configuration.

Configuring a Port for Link Fault RFI Support

Perform this task to put a port into a blocking state when an OAM PDU control request packet is received with the Link Fault Status flag set.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** { }
5. **exit**

DETAILED STEPS

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** *type number*

Example:

Enters interface configuration mode.

Step 4 **ethernet oam remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** { }

Example:

Sets the interface to the blocking state when a critical event occurs.

Step 5 **exit**

Example:

```
Device(config-if)# exit
```

Returns to global configuration mode.

Configuration Examples for Ethernet Operations Administration and Maintenance

The following example shows how to configure Ethernet OAM options using a template and overriding that configuration by configuring an interface. In this example, the network supports a Gigabit Ethernet interface between the customer edge device and provider edge device.

```
! Configure a global OAM template for both PE and CE configuration.
!
Device(config)# template oam
Device(config-template)# ethernet oam link-monitor symbol-period threshold low 10
Device(config-template)# ethernet oam link-monitor symbol-period threshold high 100
Device(config-template)# ethernet oam link-monitor frame window 100
Device(config-template)# ethernet oam link-monitor frame threshold low 10
Device(config-template)# ethernet oam link-monitor frame threshold high 100
Device(config-template)# ethernet oam link-monitor frame-period window 100
Device(config-template)# ethernet oam link-monitor frame-period threshold low 10
Device(config-template)# ethernet oam link-monitor frame-period threshold high 100
Device(config-template)# ethernet oam link-monitor frame-seconds window 1000
Device(config-template)# ethernet oam link-monitor frame-seconds threshold low 10
Device(config-template)# ethernet oam link-monitor frame-seconds threshold high 100
Device(config-template)# ethernet oam link-monitor receive-crc window 100
Device(config-template)# ethernet oam link-monitor receive-crc threshold high 100
Device(config-template)# ethernet oam link-monitor transmit-crc window 100
Device(config-template)# ethernet oam link-monitor transmit-crc threshold high 100

Device(config-template)# exit
!
! Enable Ethernet OAM on the CE interface
!
Device(config)#
Device(config-if)# ethernet oam
!
! Apply the global OAM template named "oam" to the interface.
!
Device(config-if)# source template oam
!
! Configure any interface-specific link monitoring commands to override the template
configuration. The following example disables the high threshold link monitoring for receive
 CRC errors.
!
Device(config-if)# ethernet oam link-monitor receive-crc threshold high none
!
! Enable Ethernet OAM on the PE interface
!
Device(config)#
Device(config-if)# ethernet oam
!
! Apply the global OAM template named "oam" to the interface.
```

```
!
Device(config-if)# source template oam
```

The following examples show how to verify various Ethernet OAM configurations and activities.

Verifying an OAM Session

The following example shows that the local OAM client, Gigabit Ethernet interface , is in session with a remote client with MAC address 0012.7fa6.a700 and OUI 00000C, which is the OUI for Cisco. The remote client is in active mode and has established capabilities for link monitoring and remote loopback for the OAM session.

```
Device# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval
  Local                         Remote
Interface       MAC Address    OUI    Mode    Capability
 Gi6/1/1       0012.7fa6.a700 00000C active      L R
```

Verifying OAM Discovery Status

The following example shows how to verify OAM discovery status of a local client and a remote peer:

```
Device#

Local client
------------
  Administrative configurations:
    Mode:              active
    Unidirection:      not supported
    Link monitor:      supported (on)
    Remote loopback:   not supported
    MIB retrieval:     not supported
    Mtu size:          1500
  Operational status:
Port status:       operational
    Loopback status:   no loopback
    PDU permission:    any
    PDU revision:      1
Remote client
-------------
  MAC address: 0030.96fd.6bfa
  Vendor(oui): 0x00 0x00 0x0C (cisco)
  Administrative configurations:

   Mode:              active
   Unidirection:      not supported
   Link monitor:      supported
   Remote loopback:   not supported
   MIB retrieval:     not supported
   Mtu size:          1500
```

Verifying Information OAMPDU and Fault Statistics

The following example shows how to verify statistics for information OAM PDUs and local and remote faults:

```
Device#

Counters:
```

```
---------
Information OAMPDU Tx                   : 588806
Information OAMPDU Rx                   : 988
Unique Event Notification OAMPDU Tx     : 0
Unique Event Notification OAMPDU Rx     : 0
Duplicate Event Notification OAMPDU TX  : 0
Duplicate Event Notification OAMPDU RX  : 0
Loopback Control OAMPDU Tx              : 1
Loopback Control OAMPDU Rx              : 0
Variable Request OAMPDU Tx              : 0
Variable Request OAMPDU Rx              : 0
Variable Response OAMPDU Tx             : 0
Variable Response OAMPDU Rx             : 0
Cisco OAMPDU Tx                         : 4
Cisco OAMPDU Rx                         : 0
Unsupported OAMPDU Tx                   : 0
Unsupported OAMPDU Rx                   : 0
Frames Lost due to OAM                  : 0
Local Faults:
-------------
0 Link Fault records
2 Dying Gasp records
Total dying gasps       : 4
Time stamp              : 00:30:39
Total dying gasps       : 3
Time stamp              : 00:32:39
0 Critical Event records
Remote Faults:
--------------
0 Link Fault records
0 Dying Gasp records
0 Critical Event records
Local event logs:
-----------------
0 Errored Symbol Period records
0 Errored Frame records
0 Errored Frame Period records
0 Errored Frame Second records
Remote event logs:
------------------
0 Errored Symbol Period records
0 Errored Frame records
0 Errored Frame Period records
0 Errored Frame Second records
```

Verifying Link Monitoring Configuration and Status

The following example shows how to verify link monitoring configuration and status on the local client. The highlighted Status field in the example shows that link monitoring status is supported and enabled (on).

```
Device#

General
-------
  Mode:                  active
  PDU max rate:          10 packets per second
  PDU min rate:          1 packet per 1 second
  Link timeout:          5 seconds
  High threshold action: no action
Link Monitoring
---------------
  Status: supported (on)
  Symbol Period Error
```

```
    Window:              1 million symbols
    Low threshold:       1 error symbol(s)
    High threshold:      none
  Frame Error
    Window:              10 x 100 milliseconds
    Low threshold:       1 error frame(s)
    High threshold:      none
Frame Period Error
    Window:              1 x 100,000 frames
    Low threshold:       1 error frame(s)
    High threshold:      none
  Frame Seconds Error
    Window:              600 x 100 milliseconds
    Low threshold:       1 error second(s)
    High threshold:      none
```

Verifying Status of a Remote OAM Client

The following example shows that the local client interface Gi6/1/1 is connected to a remote client. Note the values in the Mode and Capability fields.

```
Device# show ethernet oam summary
Symbols:          * - Master Loopback State,  # - Slave Loopback State
Capability codes: L - Link Monitor,  R - Remote Loopback
                  U - Unidirection,  V - Variable Retrieval
  Local                         Remote
Interface       MAC Address    OUI    Mode    Capability
 Gi6/1/1       0012.7fa6.a700 00000C active      L R
```

Additional References

Related Documents

Related Topic	Document Title
Ethernet CFM	“Configuring Ethernet Connectivity Fault Management in a Service Provider Network” module in the *Carrier Ethernet Configuration Guide*
NSF SSO Support in 802.3ah OAM	“Configuring Stateful Switchover” module in the *High Availability Configuration Guide* and “Configuring Nonstop Forwarding” in the *High Availability Configuration Guide*
ISSU Support in 802.3ah OAM	“Configuring In Service Software Upgrades" module in the *High Availability Configuration Guide*
Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Configuring CFM over an EFP Interface with the Cross Connect feature on the Cisco ASR 903 Router	*Configuring the CFM over EFP Interface with Cross Connect Feature*

Related Topic	Document Title
Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router	*Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router*

Standards

Standard	Title
IEEE Draft P802.3ah/D3.3	*Ethernet in the First Mile - Amendment*
IETF VPLS OAM	*L2VPN OAM Requirements and Framework*
ITU-T	*ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

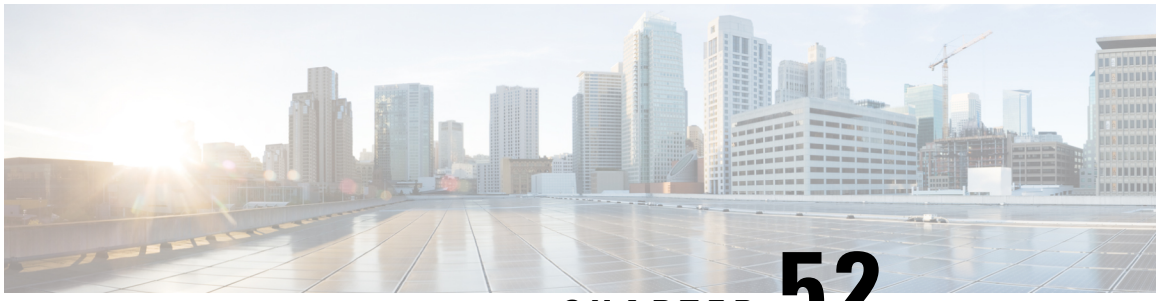
Feature Information for Using Ethernet Operations Administration and Maintenance

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 62: Feature Information for Using Ethernet Operations, Administration, and Maintenance

Feature Name	Releases	Feature Information
Ethernet Operations, Administration, and Maintenance	12.4(15)T	Ethernet OAM is a protocol for installing, monitoring, and troubleshooting metro Ethernet networks and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the OSI model. The OAM features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions. The Ethernet Operations, Administration, and Maintenance feature was integrated into Cisco IOS Release 12.4(15)T. The following commands were introduced or modified: **clear ethernet oam statistics, debug ethernet oam, ethernet oam, ethernet oam link-monitor frame, ethernet oam link-monitor frame-period, ethernet oam link-monitor frame-seconds, ethernet oam link-monitor high-threshold action, ethernet oam link-monitor on, ethernet oam link-monitor receive-crc, ethernet oam link-monitor supported, ethernet oam link-monitor symbol-period, ethernet oam link-monitor transmit-crc, ethernet oam remote-loopback, ethernet oam remote-loopback (interface), show ethernet oam discovery, show ethernet oam statistics, show ethernet oam status, show ethernet oam summary, source template (eoam), template (eoam)**.



CHAPTER 52

Configuring Ethernet Connectivity Fault Management in a Service Provider Network

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

The advent of Ethernet as a MAN and WAN technology imposes a new set of OAM requirements on Ethernet's traditional operations, which were centered on enterprise networks only. The expansion of Ethernet technology into the domain of service providers, where networks are substantially larger and more complex than enterprise networks and the user base is wider, makes operational management of link uptime crucial. More importantly, the timeliness in isolating and responding to a failure becomes mandatory for normal day-to-day operations, and OAM translates directly to the competitiveness of the service provider.

Prerequisites for Configuring Ethernet CFM in a Service Provider Network

Business Requirements

- Network topology and network administration have been evaluated.
- Business and service policies have been established.

Restrictions for Configuring Ethernet CFM in a Service Provider Network

- CFM loopback messages will not be confined within a maintenance domain according to their maintenance level. The impact of not having CFM loopback messages confined to their maintenance levels occurs at these levels:
  - Architecture—CFM layering is violated for loopback messages.
  - Deployment—A user may potentially misconfigure a network and have loopback messages succeed.
  - Security—A malicious device that recognizes devices' MAC addresses and levels may potentially explore a network topology that should be transparent.
- CFM is not fully supported on a Multiprotocol Label Switching (MPLS) provider edge (PE) device. There is no interaction between CFM and an Ethernet over MPLS (EoMPLS) pseudowire.
- CFM configuration is not supported on an EtherChannel in FastEthernet Channel (FEC) mode.
- QinQ encapsulation is not supported on the Cisco ASR 1000 Series Aggregation Services Router for CFM for routed subinterfaces.

Information About Configuring Ethernet CFM in a Service Provider Network

Ethernet CFM

Ethernet CFM is an end-to-end per-service-instance Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End to end can be PE to PE or CE to CE. A service can be identified as a service provider VLAN (S-VLAN) or an EVC service.

Being an end-to-end technology is the distinction between CFM and other metro-Ethernet OAM protocols. For example, MPLS, ATM, and SONET OAM help in debugging Ethernet wires but are not always end-to-end. 802.3ah OAM is a single-hop and per-physical-wire protocol. It is not end to end or service aware.

Troubleshooting carrier networks offering Ethernet Layer 2 services is challenging. Customers contract with service providers for end-to-end Ethernet service and service providers may subcontract with operators to provide equipment and networks. Compared to enterprise networks, where Ethernet traditionally has been implemented, these constituent networks belong to distinct organizations or departments, are substantially larger and more complex, and have a wider user base. Ethernet CFM provides a competitive advantage to service providers for which the operational management of link uptime and timeliness in isolating and responding to failures is crucial to daily operations.

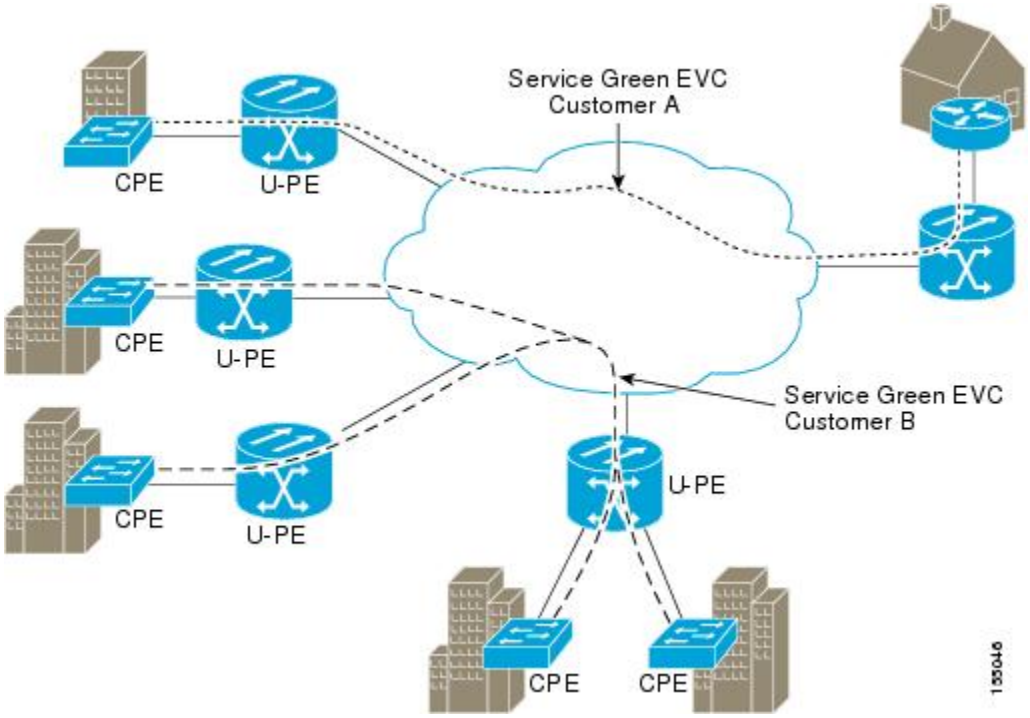
Benefits of Ethernet CFM

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks

- Competitive advantage for service providers
- Supports both distribution and access network environments with the outward facing MEPs enhancement

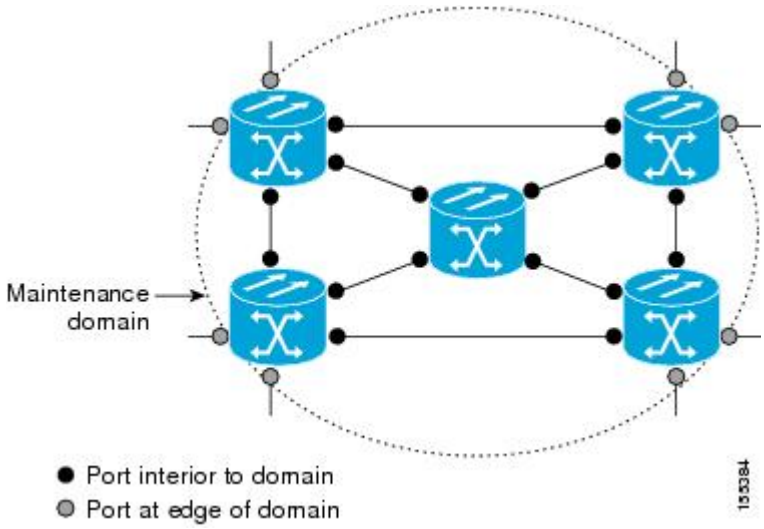
Customer Service Instance

A customer service instance is an Ethernet virtual connection (EVC), which is identified by an S-VLAN within an Ethernet island, and is identified by a globally unique service ID. A customer service instance can be point-to-point or multipoint-to-multipoint. The figure below shows two customer service instances. Service Instance Green is point to point; Service Instance Blue is multipoint to multipoint.



Maintenance Domain

A maintenance domain is a management space for the purpose of managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary. The figure below illustrates a typical maintenance domain.

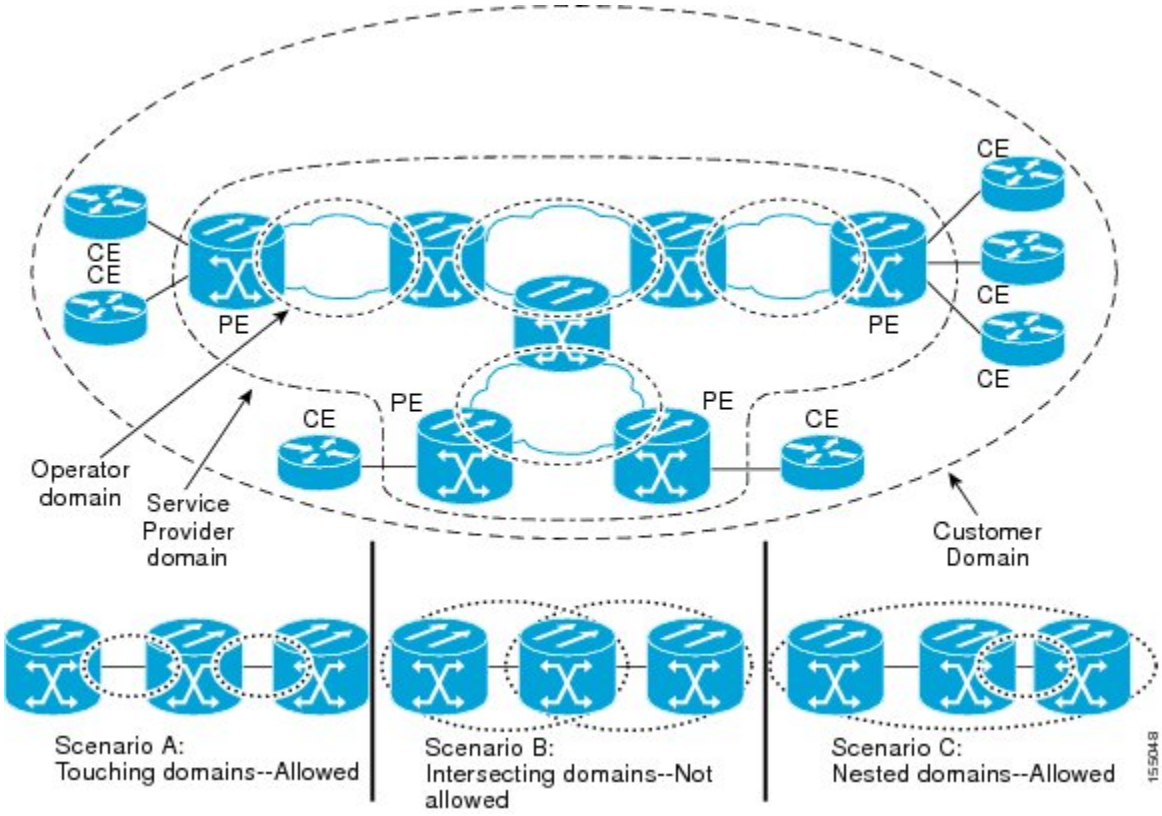


A unique maintenance level in the range of 0 to 7 is assigned to each domain by a network administrator. Levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallels the structure of customer, service provider, and operator. The larger the domain, the higher the level value. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains between them in size. All levels of the hierarchy must operate together.

Domains should not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business model where a service provider contracts with one or more operators to provide Ethernet service to a customer. Each operator would have its own maintenance domain and the service provider would define its domain—a superset of the operator domains. Furthermore, the customer has its own end-to-end domain which is in turn a superset of the service provider domain. Maintenance levels of various nesting domains should be communicated among the administering organizations. For example, one approach would be to have the service provider assign maintenance levels to operators.

CFM exchanges messages and performs operations on a per-domain basis. For example, running CFM at the operator level does not allow discovery of the network by the higher provider and customer levels.

Network designers decide on domains and configurations. The figure below illustrates a hierarchy of operator, service provider, and customer domains and also illustrates touching, intersecting, and nested domains.



Maintenance Point

A maintenance point is a demarcation point on an interface (port) that participates in CFM within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. Two classes of maintenance points exist, MEPs and MIPs.

Maintenance Endpoints

Maintenance endpoints (MEPs) have the following characteristics:

- Per maintenance domain (level) and service (S-VLAN or EVC)
- At the edge of a domain, define the boundary
- Within the bounds of a maintenance domain, confine CFM messages
- When configured to do so, proactively transmit Connectivity Fault Management (CFM) continuity check messages (CCMs)
- At the request of an administrator, transmit traceroute and loopback messages

Inward Facing MEPs

Inward facing means the MEP communicates through the Bridge Relay function and uses the Bridge-Brain MAC address. An inward facing MEP performs the following functions:

- Sends and receives CFM frames at its level through the relay function, not via the wire connected to the port on which the MEP is configured.
- Drops all CFM frames at its level (or lower level) that come from the direction of the wire.
- Processes all CFM frames at its level coming from the direction of the relay function.
- Drops all CFM frames at a lower level coming from the direction of the relay function.
- Transparently forwards all CFM frames at its level or a higher level, independent of whether they come in from the relay function side or the wire side.

Note A MEP of level L (where L is less than 7) requires a MIP of level M > L on the same port; hence, CFM frames at a level higher than the level of the MEP will be catalogued by this MIP.

- If the port on which the inward MEP is configured is blocked by Spanning-Tree Protocol, the MEP can no longer transmit or receive CFM messages.

Outward Facing MEPs for Port Channels

Outward facing means that the MEP communicates through the wire. Outward facing MEPs can be configured on port channels (using cross connect functionality). A MIP configuration at a level higher than the level of the outward facing MEP is not required.

Outward facing MEPs on port channels use the Bridge-Brain MAC address of the first member link. When port channel members change, the identities of outward facing MEPs do not have to change.

An outward facing MEP performs the following functions:

- Sends and receives CFM frames at its level via the wire connected to the port where the MEP is configured.
- Drops all CFM frames at its level (or at a lower level) that come from the direction of the relay function.
- Processes all CFM frames at its level coming from the direction of the wire.
- Drops all CFM frames at a lower level coming from the direction of the wire.
- Transparently forwards all CFM frames at levels higher than the level of the outward facing MEP, independent of whether they come in from the relay function side or the wire side.
- If the port on which the outward MEP is configured is blocked by the Spanning-Tree Protocol, the MEP can still transmit and receive CFM messages via the wire.

Maintenance Intermediate Points

MIPs have the following characteristics:

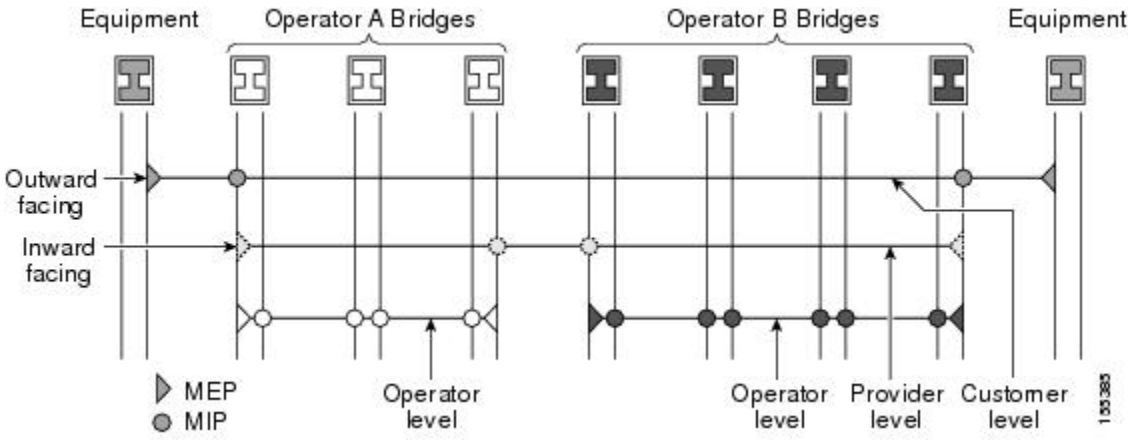
- Per maintenance domain (level) and for all S-VLANs enabled or allowed on a port.
- Internal to a domain, not at the boundary.
- CFM frames received from MEPs and other MIPs are cataloged and forwarded, using both the wire and the relay function.

- All CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or relay function.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or relay function.
- MIPs respond only when triggered by CFM traceroute and loopback messages.
- Bridge-Brain MAC addresses are used.

If the port on which a MIP is configured is blocked by Spanning-Tree Protocol, the MIP cannot receive CFM messages or relay them toward the relay function side. The MIP can, however, receive and respond to CFM messages from the wire.

A MIP has only one level associated with it and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.

The figure below illustrates MEPs and MIPs at the operator, service provider, and customer levels.



CFM Messages

CFM uses standard Ethernet frames. CFM frames are distinguishable by EtherType and for multicast messages by MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers can support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to an S-VLAN (PE-VLAN or Provider-VLAN). Three types of messages are supported:

- Continuity Check
- Loopback
- Traceroute

Continuity Check Messages

CFM CCMs are heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain and S-VLAN.

CFM CCMs have the following characteristics:

- Transmitted at a configurable periodic interval by MEPs. The interval can be from 10 seconds to 65535 seconds, the default is 30.
- Contains a configurable hold-time value to indicate to the receiver the validity of the message. The default is 2.5 times the transmit interval.
- Catalogued by MIPs at the same maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Carry the status of the port on which the MEP is configured.

Loopback Messages

CFM loopback messages are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

A CFM loopback message can be generated on demand using the CLI. The source of a loopback message must be a MEP; the destination may be a MEP or a MIP. CFM loopback messages are unicast; replies to loopback messages also are unicast. CFM loopback messages specify the destination MAC address, VLAN, and maintenance domain.

Traceroute Messages

CFM traceroute messages are multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

Traceroute messages include the destination MAC address, VLAN, and maintenance domain and they have Time To Live (TTL) to limit propagation within the network. They can be generated on demand using the CLI. Traceroute messages are multicast; reply messages are unicast.

Cross-Check Function

The cross-check function is a timer-driven post-provisioning service verification between dynamically discovered MEPs (via CCMs) and expected MEPs (via configuration) for a service. The cross-check function verifies that all endpoints of a multipoint or point-to-point service are operational. The function supports notifications when the service is operational; otherwise it provides alarms and notifications for unexpected endpoints or missing endpoints.

The cross-check function is performed one time. You must initiate the cross-check function from the CLI every time you want a service verification.

SNMP Traps

The support provided by the Cisco software implementation of CFM traps is Cisco proprietary information. MEPs generate two types of Simple Network Management Protocol (SNMP) traps, continuity check (CC) traps and cross-check traps.

CC Traps

- MEP up—Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down—Sent when a timeout or last gasp event occurs.
- Cross-connect—Sent when a service ID does not match the VLAN.
- Loop—Sent when a MEP receives its own CCMs.
- Configuration error—Sent when a MEP receives a continuity check with an overlapping MPID.

Cross-Check Traps

- Service up—Sent when all expected remote MEPs are up in time.
- MEP missing—Sent when an expected MEP is down.
- Unknown MEP—Sent when a CCM is received from an unexpected MEP.

Ethernet CFM and Ethernet OAM Interaction

To understand how CFM and OAM interact, you should understand the following concepts:

Ethernet Virtual Circuit

An EVC as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by a CE device either to find an alternative path in to the service provider network or in some cases, to fall back to a backup path over Ethernet or over another alternative service such as ATM.

OAM Manager

The OAM manager is an infrastructure element that streamlines interaction between OAM protocols. The OAM manager requires two interworking OAM protocols, in this case Ethernet CFM and Ethernet OAM. Interaction is unidirectional from the OAM manager to the CFM protocol and the only information exchanged is the user network interface (UNI) port status. Additional port status values available include

- REMOTE_EE—Remote excessive errors
- LOCAL_EE—Local excessive errors
- TEST—Either remote or local loopback

After CFM receives the port status, it communicates that status across the CFM domain.

CFM over Bridge Domains

Connectivity Fault Management (CFM) over bridge domains allows untagged CFM packets to be associated with a maintenance end point (MEP). An incoming untagged customer CFM packet has an EtherType of CFM and is mapped to an Ethernet virtual circuit (EVC) or bridge domain based on the encapsulation configured on the Ethernet flow point (EFP). The EFP is configured specifically to recognize these untagged packets.

An EFP is a logical demarcation point of an EVC on an interface and can be associated with a bridge domain. The VLAN ID is used to match and map traffic to the EFP. VLAN IDs have local significance per port similar to an ATM virtual circuit. CFM is supported on a bridge domain associated with an EFP. The association between the bridge domain and the EFP allows CFM to use the encapsulation on the EFP. All EFPs in the same bridge domain form a broadcast domain. The bridge domain ID determines the broadcast domain.

The distinction between a VLAN port and the EFP is the encapsulation. VLAN ports use a default dot1q encapsulation. For EFPs, untagged, single tagged, and double tagged encapsulation exists with dot1q and IEEE dot1ad EtherTypes. Different EFPs belonging to the same bridge domain can use different encapsulations.

Both up MEP, down MEP and MIP are supported. If an up MEP is configured under an EFP within a bridge domain, CFM messages would be routed into the bridge, and the rest members of the same bridge domain would be able to receive messages from this MEP. If a down MEP is configured, the messages will not goes into the bridge domain.

HA Features Supported by CFM

In access and service provider networks using Ethernet technology, High Availability (H)A is a requirement, especially on Ethernet OAM components that manage EVC connectivity. End-to-end connectivity status information is critical and must be maintained on a hot standby Route Switch Processor (RSP).

Note A hot standby Route Switch Processor (RSP) has the same software image as the active RSP and supports synchronization of protocol and application state information between RSPs for supported features and protocols.

End-to-end connectivity status is maintained on the customer edge (CE), provider edge (PE), and access aggregation PE (uPE) network nodes based on information received by protocols such as Connectivity Fault Management (CFM) and 802.3ah. This status information is used to either stop traffic or switch to backup paths when an EVC is down.

Every transaction involves either accessing or updating data among various databases. If the database is synchronized across active and standby modules, the modules are transparent to clients.

The Cisco infrastructure provides various component application program interfaces (APIs) that help to maintain a hot standby RSP. Metro Ethernet HA clients HA/ISSU, CFM HA/ISSU, and 802.3ah HA/ISSU interact with these components, update the database, and trigger necessary events to other components.

Benefits of CFM HA

- Elimination of network downtime for Cisco software image upgrades, allowing for faster upgrades.
- Elimination of resource scheduling challenges associated with planned outages and late night maintenance windows.

- Accelerated deployment of new services and applications and facilitation of faster implementation of new features.
- Reduced operating costs due to outages while delivering higher service levels.
- CFM updates its databases and controls its own HA messaging and versioning, and this control facilitates maintenance.

CFM HA in a Metro Ethernet Network

A standalone Connectivity Fault Management (CFM) implementation does not have explicit high availability (HA) requirements. When CFM is implemented on a customer edge (CE) or provider edge (PE), CFM must maintain the Ethernet virtual circuit (EVC) state, which requires HA because the EVC state is critical in maintaining end-to-end connectivity. CFM configures the platform with maintenance level, domain, and maintenance point, learns the remote maintenance point information, and maps it to the appropriate EVC. CFM then aggregates data received from all remote ports; consequently HA requirements vary for CE and PE.

The CE receives the EVC ID, associated customer VLANs, UNI information, EVC state, and remote UNI ID and state from the MEN. The CE relies on the EVC state to send or stop traffic to the MEN.

The PE has EVC configuration and associated customer VLAN information and derives the EVC state and remote UNI from CFM.

Note PEs and CEs running 802.3ah OAM must maintain the port state so peers are not affected by a switchover. This information is also sent to remote nodes in CFM CC messages.

NSF SSO Support in CFM 802.1ag 1.0d

The redundancy configurations Stateful Switchover (SSO) and Nonstop Forwarding (NSF) are both supported in Ethernet Connectivity Fault Management (CFM) and are automatically enabled. A switchover from an active to a standby Route Switch Processor (RSP) occurs when the active RSP fails, is removed from the networking device, or is manually taken down for maintenance. NSF interoperates with the SSO feature to minimize network downtime following a switchover. The primary function of Cisco NSF is to continue forwarding IP packets following an RSP switchover.

For detailed information about SSO, see the "Configuring Stateful Switchover" module of the *High Availability Configuration Guide*. For detailed information about the NSF feature, see the "Configuring Cisco Nonstop Forwarding" module of the *High Availability Configuration Guide*.

ISSU Support in CFM 802.1ag 1.0d

In Service Upgrades (ISSUs) allow you to perform a Cisco software upgrade or downgrade without disrupting packet flow. Connectivity Fault Management (CFM) performs a bulk update and a runtime update of the continuity check database to the standby Route Switch Processor (RSP), including adding, deleting, or updating a row. This checkpoint data requires ISSU capability to transform messages from one release to another. All the components that perform active RSP to standby RSP updates using messages require ISSU support.

ISSU is automatically enabled in CFM and lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. For detailed information

about ISSU, see the "Performing an In Service Software Upgrade " module of the *High Availability Configuration Guide*.

How to Set Up Ethernet CFM in a Service Provider Network

Designing CFM Domains

Note To have an operator, service provider, or customer domain is optional. A network may have a single domain or multiple domains. The steps listed here show the sequence when all three types of domains will be assigned.

Before you begin

- Knowledge and understanding of the network topology.
- Understanding of organizational entities involved in managing the network; for example, operators, service providers, network operations centers (NOCs), and customer service centers.
- Understanding of the type and scale of services to be offered.
- Agreement by all organizational entities on the responsibilities, roles, and restrictions for each organizational entity.
- Determination of the number of maintenance domains in the network.
- Determination of the nesting and disjoint maintenance domains.
- Assignment of maintenance levels and names to domains based on agreement between the service provider and operator or operators.
- Determination of whether the domain should be inward or outward.

SUMMARY STEPS

1. Determine operator level MIPs.
2. Determine operator level MEPs.
3. Determine service provider MIPs.
4. Determine service provider MEPs.
5. Determine customer MIPs.
6. Determine customer MEPs.

DETAILED STEPS

Step 1 Determine operator level MIPs.

Follow these steps:

- Starting at lowest operator level domain, assign a MIP at every interface internal to the operator network to be visible to CFM.
- Proceed to next higher operator level and assign MIPs.
- Verify that every port that has a MIP at a lower level does not have maintenance points at a higher level.
- Repeat steps a through d until all operator MIPs are determined.

Step 2 Determine operator level MEPs.

Follow these steps:

- Starting at the lowest operator level domain, assign a MEP at every UNI that is part of a service instance.
- Assign a MEP at the network to network interface (NNI) between operators, if there is more than one operator.
- Proceed to next higher operator level and assign MEPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should have either a MIP or MEP at a higher level.

Step 3 Determine service provider MIPs.

Follow these steps:

- Starting at the lowest service provider level domain, assign service provider MIPs at the NNI between operators (if more than one).
- Proceed to next higher service provider level and assign MIPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should not have either a MIP or a MEP at a higher level.

Step 4 Determine service provider MEPs.

Follow these steps:

- Starting at the lowest service provider level domain, assign a MEP at every UNI that is part of a service instance.
- Proceed to next higher service provider level and assign MEPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should have either a MIP or a MEP at a higher level.

Step 5 Determine customer MIPs.

Customer MIPs are allowed only on the UNIs at the uPEs if the service provider allows the customer to run CFM. Otherwise, the service provider can configure Cisco devices to block CFM frames.

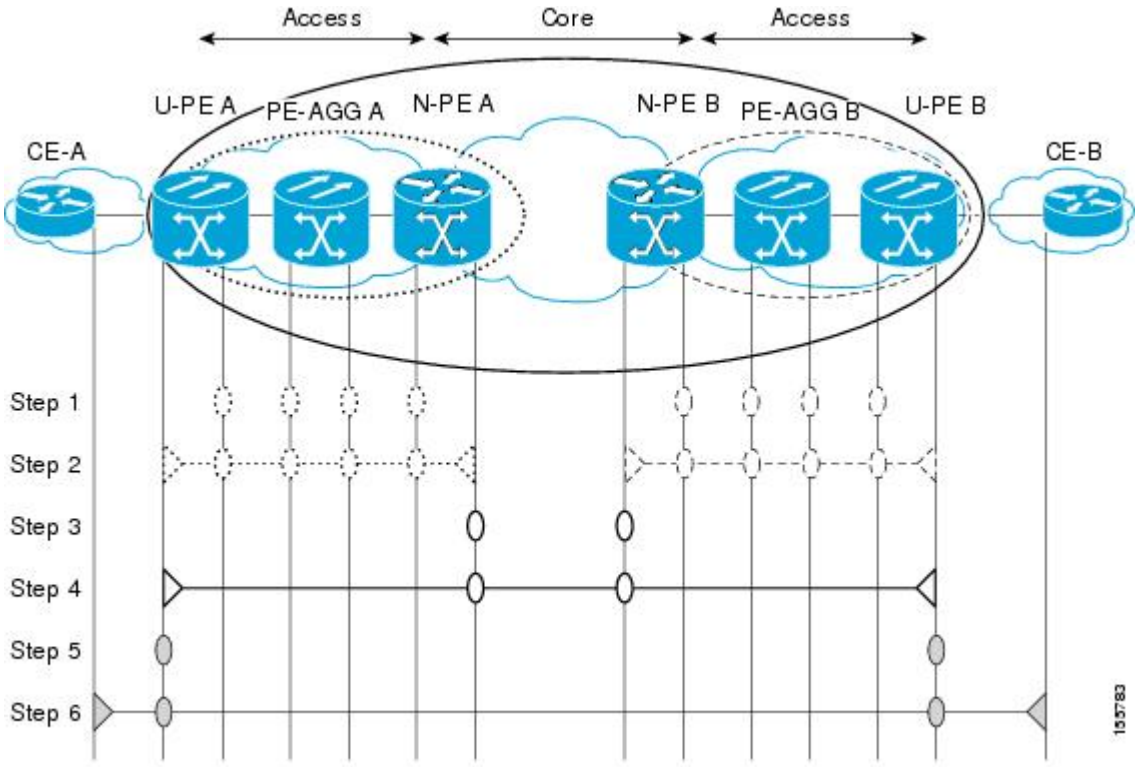
- Configure a MIP on every uPE, at the UNI port, in the customer maintenance domain.
- Ensure the MIPs are at a maintenance level that is at least one higher than the highest level service provider domain.

Step 6 Determine customer MEPs.

Customer MEPs are on customer equipment. Assign an outward facing MEP within an outward domain at the appropriate customer level at the handoff between the service provider and the customer.

Examples

The figure below shows an example of a network with a service provider and two operators, A and B. Three domains are to be established to map to each operator and the service provider. In this example, for simplicity we assume that the network uses Ethernet transport end to end. CFM, however, can be used with other transports.



What to Do Next

After you have defined the Ethernet CFM domains, configure Ethernet CFM functionality by first provisioning the network and then provisioning service.

Configuring Ethernet CFM

Configuring Ethernet CFM consists of the following tasks:

Provisioning the Network

Provisioning the Network on the CE-A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
15. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
16. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.

	Command or Action	Purpose
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.

	Command or Action	Purpose
Step 14	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM continuity check events.
Step 15	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM continuity check events in relation to the cross-check operation between statically configured MEPS and those learned via CCMs.
Step 16	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the U-PE A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** { *level* }
19. **exit**
20. **exit**
21. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]

22. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
23. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:**	Returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-ecfm)# exit`	
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mip level** { *level* } **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.

	Command or Action	Purpose
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 22	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 23	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the PE-AGG A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **interface** *type number*
12. **service instance** *id* **ethernet** [*evc-name*]
13. **encapsulation** *encapsulation-type*
14. **bridge-domain** *bridge-id*
15. **cfm mip level** *level*
16. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 65`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns the CLI to global configuration mode.

	Command or Action	Purpose
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 12	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 13	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 14	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 15	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 16	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the N-PE A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **ethernet cfm global**
9. **ethernet cfm traceroute cache**
10. **ethernet cfm traceroute cache size** *entries*
11. **ethernet cfm traceroute cache hold-time** *minutes*
12. **interface** *type number*

13. **service instance** *id* **ethernet** [*evc-name*]
14. **encapsulation** *encapsulation-type*
15. **bridge-domain** *bridge-id*
16. **cfm mip level** *level*
17. **exit**
18. **exit**
19. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
20. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
21. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.

	Command or Action	Purpose
Step 8	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 9	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 10	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 11	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 12	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 13	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 14	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 15	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 16	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 17	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.

	Command or Action	Purpose
Step 18	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 19	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 20	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 21	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the CE-B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
15. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
16. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.

	Command or Action	Purpose
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 15	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 16	**end** **Example:** `Device(config)# end#`	Returns to privileged EXEC mode.

Provisioning the Network on the U-PE B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**

11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** *level*
19. **exit**
20. **exit**
21. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
22. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
23. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.

	Command or Action	Purpose
Step 18	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 22	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 23	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the PE-AGG B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **interface** *type number*
12. **service instance** *id* **ethernet** [*evc-name*]

13. **encapsulation** *encapsulation-type*
14. **bridge-domain** *bridge-id*
15. **cfm mip level** *level*
16. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 65`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 12	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 13	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 14	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 15	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 16	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning the Network on the N-PE B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*

15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** *level*
19. **exit**
20. **exit**
21. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
22. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**]
23. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.

	Command or Action	Purpose
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.

	Command or Action	Purpose
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 22	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown** | **mep-missing** | **service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown mep-missing service-up`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 23	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Provisioning Service

Provisioning Service on the CE-A

Perform this task to set up service for Ethernet CFM. Optionally, when this task is completed, you may configure and enable the cross-check function. To perform this optional task, see "Configuring and Enabling Cross-Checking for an Inward Facing MEP on the U PE-A".

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**

11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mep domain** *domain-name* **mpid** *id*
19. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.

	Command or Action	Purpose
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.

	Command or Action	Purpose
Step 19	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the U-PE A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mep domain** *domain-name* **mpid** *id*
19. **exit**
20. **exit**
21. **interface** *type number*
22. **service instance** *id* **ethernet** [*evc-name*]
23. **encapsulation** *encapsulation-type*
24. **bridge-domain** *bridge-id*
25. **cfm mip level** *level*
26. **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 domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.

	Command or Action	Purpose
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 22	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

	Command or Action	Purpose
Step 23	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 24	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 25	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 26	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the PE-AGG A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **interface** *type number*
12. **service instance** *id* **ethernet** [*evc-name*]
13. **encapsulation** *encapsulation-type*
14. **bridge-domain** *bridge-id*
15. **cfm mip level** *level*
16. **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 domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 65`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 12	**service instance** *id* **ethernet** [*evc-name*] **Example:**	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

	Command or Action	Purpose
	`Device(config-if)# service instance 333 ethernet evc1`	
Step 13	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 14	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 15	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 16	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the N-PE A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** *level*
19. **exit**
20. **exit**
21. **interface** *type number*
22. **service instance** *id* **ethernet** [*evc-name*]
23. **encapsulation** *encapsulation-type*

24. **bridge-domain** *bridge-id*
25. **cfm mep domain** *domain-name* **mpid** *id*
26. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 21	**interface** *type number* **Example:**	Specifies an interface.
Step 22	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 23	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 24	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 25	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.
Step 26	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the CE-B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mep domain** *domain-name* **mpid** *id*

19. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:**	Enables CFM processing globally on the device.

	Command or Action	Purpose
	`Device(config)# ethernet cfm global`	
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.
Step 19	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the U-PE B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**

5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** *level*
19. **exit**
20. **exit**
21. **interface** *type number*
22. **service instance** *id* **ethernet** [*evc-name*]
23. **encapsulation** *encapsulation-type*
24. **bridge-domain** *bridge-id*
25. **cfm mep domain** *domain-name* **mpid** *id*
26. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.

	Command or Action	Purpose
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

	Command or Action	Purpose
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 22	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 23	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 24	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 25	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.
Step 26	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the PE-AGG B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **interface** *type number*
12. **service instance** *id* **ethernet** [*evc-name*]
13. **encapsulation** *encapsulation-type*
14. **bridge-domain** *bridge-id*
15. **cfm mip level** *level*
16. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).

	Command or Action	Purpose
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 65`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 12	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 13	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 14	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 15	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 16	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Provisioning Service on the N-PE B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **continuity-check**
6. **continuity-check** [**interval** *cc-interval*]
7. **exit**
8. **mep archive-hold-time** *minutes*
9. **exit**
10. **ethernet cfm global**
11. **ethernet cfm traceroute cache**
12. **ethernet cfm traceroute cache size** *entries*
13. **ethernet cfm traceroute cache hold-time** *minutes*
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-name*]
16. **encapsulation** *encapsulation-type*
17. **bridge-domain** *bridge-id*
18. **cfm mip level** *level*
19. **exit**
20. **exit**
21. **interface** *type number*
22. **service instance** *id* **ethernet** [*evc-name*]
23. **encapsulation** *encapsulation-type*
24. **bridge-domain** *bridge-id*
25. **cfm mep domain** *domain-name* **mpid** *id*
26. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.

	Command or Action	Purpose
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**continuity-check** **Example:** `Device(config-ecfm-srv)# continuity-check`	Configures the transmission of continuity check messages (CCMs).
Step 6	**continuity-check** [**interval** *cc-interval*] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the per-service parameters and sets the interval at which CCMs are transmitted.
Step 7	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns to Ethernet connectivity fault management configuration mode.
Step 8	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 9	**exit** **Example:** `Device(config-ecfm)# exit`	Returns to global configuration mode.
Step 10	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 11	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 12	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 13	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.

	Command or Action	Purpose
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 16	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 17	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 18	**cfm mip level** *level* **Example:** `Device(config-if-srv)#cfm mip level 4`	Creates a MIP and sets the maintenance level number.
Step 19	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.
Step 20	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 21	**interface** *type number* **Example:**	Specifies an interface.
Step 22	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Device(config-if)# service instance 333 ethernet evc1`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.
Step 23	**encapsulation** *encapsulation-type* **Example:**	Sets the encapsulation method used by the interface.
Step 24	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Binds a service instance to a bridge domain instance.
Step 25	**cfm mep domain** *domain-name* **mpid** *id* **Example:** `Device(config-if-srv)# cfm mep domain L4 mpid 4001`	Configures the MEP domain and the ID.

	Command or Action	Purpose
Step 26	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.

Configuring and Enabling the Cross-Check Function

Configuring and Enabling Cross-Checking for an Inward Facing MEP on the U PE-A

Perform this task to configure and enable cross-checking for an inward facing MEP. This task requires you to configure and enable cross-checking on two devices. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]
5. **exit**
6. **ethernet cfm mep crosscheck start-delay** *delay*
7. **exit**
8. **ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]}

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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain ServiceProvider level 4`	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*] **Example:** `Device(config-ether-cfm)# mep crosscheck mpid 402 vlan 100`	Statically defines a remote MEP on a specified VLAN within the domain.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit#`	Returns to global configuration mode.
Step 6	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]} **Example:** `Device# ethernet cfm mep crosscheck enable level 4 vlan 100`	Enables cross-checking between remote MEPs in the domain and MEPs learned through CCMs.

Example

The following example configures cross-checking on an inward facing MEP (U-PE A):

```
U-PE A
ethernet cfm domain ServiceProvider level 4
mep crosscheck mpid 402 vlan 100
!
ethernet cfm mep crosscheck start-delay 60
```

The following example enables cross-checking on an inward facing MEP (U-PE A):

```
U-PE A
U-PEA# ethernet cfm mep crosscheck enable level 4 vlan 100
```

Configuring and Enabling Cross-Checking for an Inward Facing MEP on the U PE-B

Perform this task to configure and enable cross-checking for an inward facing MEP. This task requires you to configure and enable cross-checking on two devices. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]
5. **exit**
6. **ethernet cfm mep crosscheck start-delay** *delay*
7. **exit**

8. **ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]}

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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain ServiceProvider level 4`	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*] **Example:** `Device(config-ether-cfm)# mep crosscheck mpid 401 vlan 100`	Statically defines a remote MEP on a specified VLAN within the domain.
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 6	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]} **Example:** `Device# ethernet cfm mep crosscheck enable level 4 vlan 100`	Enables cross-checking between MEPs.

Example

The following example configures cross-checking on an inward facing MEP (U-PE B)

```
U-PE B
ethernet cfm domain ServiceProvider level 4
mep crosscheck mpid 401 vlan 100
!
ethernet cfm mep crosscheck start-delay 60
```

The following example enables cross-checking on an inward facing MEP (U-PE B)

```
U-PE B
U-PEB# ethernet cfm mep crosscheck enable level 4 vlan 100
```

Configuring and Enabling Cross-Checking for an Outward Facing MEP on the CE-A

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]
4. **mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]
5. **exit**
6. **ethernet cfm mep crosscheck start-delay** *delay*
7. **exit**
8. **ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]}

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	**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain Customer level 7 direction outward`	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*] **Example:**	Statically defines a remote MEP with a specified ID, VLAN, and domain.

	Command or Action	Purpose
	`Device(config-ether-cfm)# mep crosscheck mpid 702 vlan 100`	
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 6	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]} **Example:** `Device# ethernet cfm mep crosscheck enable level 7 vlan 100`	Enables cross-checking between MEPs.

Configuring and Enabling Cross-Checking for an Outward Facing MEP on the CE-B

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]
4. **mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*]
5. **exit**
6. **ethernet cfm mep crosscheck start-delay** *delay*
7. **exit**
8. **ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]}

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain Customer level 7 direction outward`	Defines an outward CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**mep crosscheck mpid** *id* **vlan** *vlan-id* [**mac** *mac-address*] **Example:** `Device(config-ether-cfm)# mep crosscheck mpid 401 vlan 100`	Statically defines a remote MEP on a VLAN within a specified domain.
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 6	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**ethernet cfm mep crosscheck** {**enable** | **disable**} **level** {*level-id* | *level-id-level-id* [,*level-id-level-id*]} **vlan** {*vlan-id* | **any** | *vlan-id-vlan-id* [,*vlan-id-vlan-id*]} **Example:** `Device# ethernet cfm mep crosscheck enable level 7 vlan 100`	Enables cross-checking between MEPs.

Configuring CFM over Bridge Domains

Perform this task to configure Ethernet CFM over bridge domains. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id* **direction outward**
4. **service** *csi-id* **evc** *evc-name*
5. **exit**
6. **ethernet cfm domain** *domain-name* **level** *level-id*
7. **exit**

8. **ethernet cfm domain** *domain-name* **level** *level-id*
9. **service** *csi-id* **evc** *evc-name*
10. **mep crosscheck mpid** *id* **evc** *evc-name* **mac** *mac-address*
11. **exit**
12. **ethernet evc** *evc-name*
13. **exit**
14. **interface** *type number*
15. **no ip address**
16. **service instance** *id* **ethernet** *evc-id*
17. **encapsulation dot1q** *vlan-id*
18. **bridge-domain** *bridge-id*
19. **cfm mep domain** *domain-name* **mpid** *mpid-value*
20. **end**
21. **configure terminal**
22. **interface** *type name*
23. **no ip address**
24. **ethernet cfm mip level** *level-id*
25. **service instance** *id* **ethernet** *evc-id*
26. **encapsulation dot1q** *vlan-id*
27. **bridge-domain** *bridge-id*
28. **cfm mep domain** *domain-name* **mpid** *mpid-value*
29. **end**
30. **configure terminal**
31. **ethernet cfm cc enable level** *level-id* **evc** *evc-name*
32. **ethernet cfm cc level any evc** *evc-name* **interval** *seconds* **loss-threshold** *num-msgs*
33. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **direction outward** **Example:**	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.

	Command or Action	Purpose
	`Device(config)# ethernet cfm domain CUSTOMER level 7 direction outward`	
Step 4	**service** *csi-id* **evc** *evc-name* **Example:** `Device(config-ether-cfm)# service customer_100 evc evc_100`	Sets a universally unique ID for a CSI within a maintenance domain.
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain MIP level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 7	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 8	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain PROVIDER level 4`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 9	**service** *csi-id* **evc** *evc-name* **Example:** `Device(config-ether-cfm)# service provider_1 evc evc_100`	Sets a universally unique ID for a CSI within a maintenance domain.
Step 10	**mep crosscheck mpid** *id* **evc** *evc-name* **mac** *mac-address* **Example:** `Device(config-ether-cfm)# mep crosscheck mpid 200 evc evc_100 mac 1010.1010.1010`	Statically defines a remote MEP within a maintenance domain.
Step 11	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 12	**ethernet evc** *evc-name* **Example:** `Device(config)# ethernet evc evc_100`	Defines an EVC and enters EVC configuration mode.
Step 13	**exit** **Example:** `Device(config-evc)# exit`	Returns to global configuration mode.
Step 14	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 15	**no ip address** **Example:** `Device(config-if)# no ip address`	Disables IP processing.
Step 16	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc_100`	Specifies an Ethernet service instance on an interface and enters service instance configuration mode.
Step 17	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 18	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Establishes a bridge domain.
Step 19	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain CUSTOMER mpid 1001`	Configures a MEP for a domain.
Step 20	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.
Step 21	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 22	**interface** *type name* **Example:**	Specifies an interface and enters interface configuration mode.
Step 23	**no ip address** **Example:** `Device(config-if)# no ip address`	Disables IP processing.
Step 24	**ethernet cfm mip level** *level-id* **Example:** `Device(config-if)# ethernet cfm mip level 7`	Provisions a MIP at a specified maintenance level on an interface.
Step 25	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc_100`	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 26	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 27	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 100`	Establishes a bridge domain.
Step 28	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain PROVIDER inward mpid 201`	Configures a MEP for a domain.
Step 29	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.
Step 30	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 31	**ethernet cfm cc enable level** *level-id* **evc** *evc-name* **Example:** `Device(config)# ethernet cfm cc enable level 0-7 evc evc_100`	Globally enables transmission of CCMs.
Step 32	**ethernet cfm cc level any evc** *evc-name* **interval** *seconds* **loss-threshold** *num-msgs* **Example:** `Device(config)# ethernet cfm cc level any evc evc_100 interval 100 loss-threshold 2`	Sets the parameters for CCMs.
Step 33	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

What to do next

Note When configuring CFM over bridge domains where the bridge-domain ID matches the vlan ID service, you must configure the vlan service and the EVC service with the same service name. The bridge-domain is associated with the EVC service. The vlan and the bridge-domain represent the same broadcast domain.

Configuring CFM Over Port Channels

Configuring UP MEP over Port Channel in L2VPN

Perform this task to configure up Maintenance End Point (MEP) over port channel in Layer 2 VPN (L2VPN). This task shows Provider Edge 1 and 2 configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm ieee**
4. **ethernet cfm global**
5. **ethernet cfm domain** *domain-name* **level** *level-id*
6. **service** *csi-id* **evc** *evc-name*
7. **continuity-check** [**inteval** *time*]
8. **exit**
9. **ethernet evc** *evc-name*
10. **pseudowire-class** *pw-class-name*
11. **encapsulation mpls**

12. **exit**
13. **interface** *type number*
14. **service instance** *id* **ethernet** *evc-id*
15. **encapsulation dot1q** *vlan-id*
16. **rewrite ingress tag pop 1 symmetric**
17. **xconnect** *peer-ip-addressvc-id* **pw-class** *pw-class-name*
18. **cfm mep domain** *domain-name* **mpid** *mpid-value*
19. *exit*
20. **ethernet cfm ieee**
21. **ethernet cfm global**
22. **ethernet cfm domain** *domain-name* **level** *level-id*
23. **service** *csi-id* **evc** *evc-name*
24. **continuity-check** [**inteval** *ime*]
25. **exit**
26. **ethernet evc** *evc-name*
27. **pseudowire-class** *pw-class-name*
28. **encapsulation mpls**
29. **exit**
30. **interface** *type number*
31. **service instance** *id* **ethernet** *evc-id*
32. **encapsulation dot1q** *vlan-id*
33. **rewrite ingress tag pop 1 symmetric**
34. **xconnect** *peer-ip-addressvc-id* **pw-class** *pw-class-name*
35. **cfm mep domain** *domain-name* **mpid** *mpid-value*

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	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 4	**ethernet cfm global** **Example:**	Enables Ethernet connectivity fault management (CFM) globally on a device.

	Command or Action	Purpose
	`Device(config)# ethernet cfm global`	
Step 5	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain CUSTOMER level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 6	**service** *csi-id* **evc** *evc-name* **Example:** `Device(config-ether-cfm)# service customer100 evc evc100`	Sets a universally unique ID for a customer service instance (CSI) within a maintenance domain.
Step 7	**continuity-check** [**inteval** *time*] **Example:** `Device(config-ether-cfm)# continuity-check interval 1s`	Enables the transmission of continuity check messages (CCMs)
Step 8	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 9	**ethernet evc** *evc-name* **Example:** `Device(config)# ethernet evc evc100`	Enables Ethernet Virtual Circuit (EVC).
Step 10	**pseudowire-class** *pw-class-name* **Example:** `Device(config-evc)# pseudowire-class vlan-xconnect`	Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
Step 11	**encapsulation mpls** **Example:** `Device(config-pw)# encapsulation mpls`	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire
Step 12	**exit** **Example:** `Device (config-ecfm-srv)# exit`	Exits Ethernet CFM configuration mode and returns to global configuration mode.
Step 13	**interface** *type number* **Example:**	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface port-channel 10`	
Step 14	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc100`	Specifies an Ethernet service instance on an interface and enters service instance configuration mode.
Step 15	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 16	**rewrite ingress tag pop 1 symmetric** **Example:** `Device(config-if-srv)#  rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 17	**xconnect** *peer-ip-addressvc-id* **pw-class** *pw-class-name* **Example:** `Device(config-if-srv)#  xconnect 10.1.1.1 100 pw-class vlan-xconnect`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 18	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain CUSTOMER mpid 1111`	Configures a MEP for a domain.
Step 19	*exit* **Example:** `Device(config-if-srv)# exit`	Exits service instance configuration mode and enters global configuration mode. **Note** The configuration for Provider Edge Device 1 (PE1) ends here. Perform the next steps for PE2 configuration.
Step 20	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 21	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables Ethernet connectivity fault management (CFM) globally on a device.

	Command or Action	Purpose
Step 22	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain CUSTOMER level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 23	**service** *csi-id* **evc** *evc-name* **Example:** `Device(config-ether-cfm)# service customer100 evc evc100`	Sets a universally unique ID for a customer service instance (CSI) within a maintenance domain.
Step 24	**continuity-check** [**inteval** *ime*] **Example:** `Device(config-ether-cfm)# continuity-check interval 1s`	Enables the transmission of continuity check messages (CCMs)
Step 25	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 26	**ethernet evc** *evc-name* **Example:** `Device(config)# ethernet evc evc_100`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 27	**pseudowire-class** *pw-class-name* **Example:** `Device(config-evc)# pseudowire-class vlan-xconnect`	Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
Step 28	**encapsulation mpls** **Example:** `Device(config-pw)# encapsulation mpls`	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire
Step 29	**exit** **Example:** `Device (config-ecfm-srv)# exit`	Exits Ethernet CFM configuration mode and returns to global configuration mode.
Step 30	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0/0/1`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 31	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc100`	Specifies an Ethernet service instance on an interface and enters service instance configuration mode.
Step 32	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 33	**rewrite ingress tag pop 1 symmetric** **Example:** `Device(config-if-srv)#  rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 34	**xconnect** *peer-ip-addressvc-id* **pw-class** *pw-class-name* **Example:** `Device(config-if-srv)#  xconnect 10.1.1.2 100 pw-class vlan-xconnect`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 35	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain CUSTOMER mpid 2222`	Configures a MEP for a domain.

Configuring UP MEP over Port Channel in VPLS

Perform this task to configure up Maintenance End Point (MEP) over port channel in VPLS. This task shows configurations for Provider Edge (PE)1 and PE2 devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm ieee**
4. **ethernet cfm global**
5. **ethernet cfm domain** *domain-name* **level** *level-id*
6. **service** *csi-id* **evc** *evc-name*
7. **continuity-check** [**inteval** *time*]
8. **exit**
9. **ethernet evc** *evc-name*
10. **exit**
11. **l2vpn vfi context** *name*

12. **vpn id** *vpn-id*
13. **evc** *evc-name*
14. **member** *ip-address* **encapsulation mpls**
15. **exit**
16. **interface** *type number*
17. **service instance** *id* **ethernet** *evc-id*
18. **encapsulation dot1q** *vlan-id*
19. **rewrite ingress tag pop 1 symmetric**
20. **cfm mep domain** *domain-name* **mpid** *mpid-value*
21. **exit**
22. **bridge-domain** *bridge-id*
23. **member** *interface-type-number* **service-instance** *service-id*
24. **member** *interface-type-number*
25. **exit**

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	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 4	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables Ethernet connectivity fault management (CFM) globally on a device.
Step 5	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain CUSTOMER level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 6	**service** *csi-id* **evc** *evc-name* **Example:**	Sets a universally unique ID for a customer service instance (CSI) within a maintenance domain.

	Command or Action	Purpose
	`Device(config-ether-cfm)# service customer100 evc evc100`	
Step 7	**continuity-check** [**inteval** *time*] **Example:** `Device(config-ether-cfm)# continuity-check interval 1s`	Enables the transmission of continuity check messages (CCMs)
Step 8	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 9	**ethernet evc** *evc-name* **Example:** `Device(config)# ethernet evc evc100`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 10	**exit** **Example:** `Device(config-evc)# exit`	Returns to global configuration mode.
Step 11	**l2vpn vfi context** *name* **Example:** `Device(config)# l2vpn vfi context vpls1`	Establishes a Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) between two or more separate networks and enters VFI configuration mode.
Step 12	**vpn id** *vpn-id* **Example:** `Device(config-vfi)# vpn id 1`	Updates a VPN ID on a Virtual Private LAN Services (VPLS) instance.
Step 13	**evc** *evc-name* **Example:** `Device(config-vfi)# evc evc100`	Configures an EVC on a VPLS instance.
Step 14	**member** *ip-address* **encapsulation mpls** **Example:** `Device(config-vfi)# member 10.1.1.1 encapsulation mpls`	Specifies the devices that form a point-to-point Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) connection.
Step 15	**exit** **Example:**	Exits VFI configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device (config-vfi)# exit`	
Step 16	**interface** *type number* **Example:** `Device(config)# interface port-channel 10`	Specifies an interface and enters interface configuration mode.
Step 17	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc100`	Specifies an Ethernet service instance on an interface and enters service instance configuration mode.
Step 18	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 19	**rewrite ingress tag pop 1 symmetric** **Example:** `Device(config-if-srv)#  rewrite ingress tag pop 1 symmetric`	Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance.
Step 20	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain CUSTOMER mpid 1001`	Configures a MEP for a domain.
Step 21	**exit** **Example:** `Device (config-if-srv)# exit`	Exits service instance configuration mode and returns to global configuration mode.
Step 22	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	Configures the components on a bridge domain and enters bridge-domain configuration mode.
Step 23	**member** *interface-type-number* **service-instance** *service-id* **Example:** `Device(config-bdomain)# member port-channel 10 service-instance 100`	Binds a service instance to a bridge domain instance.

	Command or Action	Purpose
Step 24	**member** *interface-type-number* **Example:** `Device(config-bdomain)# member vfi vpls1`	Binds a service instance to a bridge domain instance.
Step 25	**exit** **Example:** `Device (config-bdomain)# exit`	Exits bridge domain configuration mode and returns to global configuration mode.

Configuring Down MEP over Port Channel

Perform this task to configure down MEP over port channel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm ieee**
4. **ethernet cfm global**
5. **ethernet cfm domain** *domain-name* **level** *level-id*
6. **service** *csi-id* **evc** *evc-name* s **vlan** *vlan-id* **direction down**
7. **continuity-check** [**inteval** *time*]
8. **exit**
9. **ethernet evc** *evc-name*
10. **exit**
11. **interface** *type number*
12. **service instance** *id* **ethernet** *evc-id*
13. **encapsulation dot1q** *vlan-id*
14. **bridge-domain** *bridge-id*
15. **cfm mep domain** *domain-name* **mpid** *mpid-value*

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.

	Command or Action	Purpose
Step 3	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 4	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables Ethernet connectivity fault management (CFM) globally on a device.
Step 5	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain CUSTOMER level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 6	**service** *csi-id* **evc** *evc-name* s **vlan** *vlan-id* **direction down** **Example:** `Device(config-ether-cfm)# service customer_100 evc evc_100 vlan 100 direction down`	Configures a maintenance association within a maintenance domain and enter Ethernet connectivity fault management (CFM) service configuration mode.
Step 7	**continuity-check** [**inteval** *time*] **Example:** `Device(config-ether-cfm)# continuity-check interval 1s`	Enables the transmission of continuity check messages (CCMs)
Step 8	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 9	**ethernet evc** *evc-name* **Example:** `Device(config)# ethernet evc evc_100`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 10	**exit** **Example:** `Device (config-ecfm-srv)# exit`	Exits Ethernet CFM configuration mode and returns to global configuration mode.
Step 11	**interface** *type number* **Example:** `Device(config)# interface port-channel10`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 12	**service instance** *id* **ethernet** *evc-id* **Example:** `Device(config-if)# service instance 100 ethernet evc_100`	Specifies an Ethernet service instance on an interface and enters service instance configuration mode.
Step 13	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to map 802.1Q frames on an ingress interface to the appropriate service instance.
Step 14	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)#  bridge domain 100`	Configures the components on a bridge domain.
Step 15	**cfm mep domain** *domain-name* **mpid** *mpid-value* **Example:** `Device(config-if-srv)# cfm mep domain CUSTOMER mpid 2222`	Configures a MEP for a domain.

Configuring CFM Offload

Perform this task to configure Connectivity Fault Management (CFM) offload.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm ieee**
4. **ethernet cfm global**
5. **ethernet cfm domain** *domain-name* **level** *level-id*
6. **service** *csi-id* **evc** *evc-name*
7. **continuity-check** [**inteval** *time*]
8. **offload sampling** *sample*
9. **exit**

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 ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
Step 4	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables Ethernet connectivity fault management (CFM) globally on a device.
Step 5	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain CUSTOMER level 7`	Defines a CFM maintenance domain at a particular level and enters Ethernet CFM configuration mode.
Step 6	**service** *csi-id* **evc** *evc-name* **Example:** `Device(config-ether-cfm)# service customer100 evc evc100`	Sets a universally unique ID for a customer service instance (CSI) within a maintenance domain.
Step 7	**continuity-check** [**inteval** *time*] **Example:** `Device(config-ether-cfm)# continuity-check interval 3.3s`	Enables the transmission of continuity check messages (CCMs)
Step 8	**offload sampling** *sample* **Example:**	Configures offload sampling.

	Command or Action	Purpose
	`Device(config-ether-cfm)# offload sampling 1000`	**Note** ASR1000 routers can offload sessions with CCM interval of 100 milliseconds, 10 milliseconds, and 3.3 milliseconds. CCM session with 1 second interval does not get offloaded by default. To offload the CCM session with 1 second, configure the sampling rate (offload sampling). The CCM session with 10 minutes, 1 minute, and 10 seconds are not offloaded. The suggested offload sampling for each CCM interval is as follows: • 1s - 10 • 100ms - 100 • 10ms - 1000 • 3.3ms - 2000
Step 9	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.

Troubleshooting Tips

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

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

Configuring Ethernet OAM Interaction with CFM

For Ethernet OAM to function with CFM, you must configure an EVC and the OAM manager and associate the EVC with CFM. Additionally, you must use an inward facing MEP when you want interaction with the OAM manager.

Configuring the OAM Manager

Note If you configure, change, or remove a UNI service type, EVC, Ethernet service instance, or CE-VLAN configuration, all configurations are checked to ensure that UNI service types are matched with EVC configurations and Ethernet service instances are matched with CE-VLAN configurations. Configurations are rejected if the pairings do not match.

Perform this task to configure the OAM manager on a PE device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]
4. **service** *csi-id* **vlan** *vlan-id*
5. **exit**
6. **ethernet evc** *evc-id*
7. **oam protocol** {**cfm svlan** *svlan-id* **domain** *domain-name* | **ldp**}
8. **exit**
9. Repeat Steps 3 through 8 to define other CFM domains that you want OAM manager to monitor.
10. **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	**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain cstmr1 level 3`	Defines a CFM domain, sets the domain level, and enters Ethernet CFM configuration mode.
Step 4	**service** *csi-id* **vlan** *vlan-id* **Example:** `Device(config-ether-cfm)# service csi2 vlan 10`	Defines a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-ether-cfm)# exit`	Returns to global configuration mode.
Step 6	**ethernet evc** *evc-id* **Example:** `Device(config)# ethernet evc 50`	Defines an EVC and enters EVC configuration mode.
Step 7	**oam protocol** {**cfm svlan** *svlan-id* **domain** *domain-name* | **ldp**} **Example:** `Device(config-evc)# oam protocol cfm svlan 10 domain cstmr1`	Configures the EVC OAM protocol.
Step 8	**exit** **Example:** `Device(config-evc)# exit`	Returns to global configuration mode.
Step 9	Repeat Steps 3 through 8 to define other CFM domains that you want OAM manager to monitor.	—
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Enabling Ethernet OAM

The order in which the global and interface configuration commands are issued determines the configuration. The last command that is issued has precedence.

Perform this task to enable Ethernet OAM on a device or on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*]
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** *type number* **Example:**	Specifies an interface and enters interface configuration mode.
Step 4	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *num-seconds*| **mode** {**active** | **passive**} | **timeout** *seconds*] **Example:** `Device(config-if)# ethernet oam max-rate 50`	Enables Ethernet OAM on an interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Configuring Ethernet CFM in a Service Provider Network

Example: Provisioning a Network

This configuration example shows only CFM-related commands. All commands that are required to set up the data path and configure the VLANs on the device are not shown. However, it should be noted that CFM traffic will not flow into or out of the device if the VLANs are not properly configured.

```
CE-A
!
ethernet cfm domain Customer level 7
!!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
```

```
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up

U-PE A
!
ethernet cfm domain Customer level 7
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!

ethernet cfm mip level 1
!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
PE-AGG A
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
!
ethernet cfm global
!

ethernet cfm mip level 1
!

ethernet cfm mip level 1
N-PE A
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!

ethernet cfm mip level 1
!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
U-PE B
!
ethernet cfm domain Customer level 7
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
!
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
```

```
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!

ethernet cfm mip level 2
!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
PE-AGG B
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
!
ethernet cfm global
!

ethernet cfm mip level 2
!

ethernet cfm mip level 2
N-PE B
!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
!
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!

ethernet cfm mip level 2
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
CE-B
!
ethernet cfm domain Customer level 7
!!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!!
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

Example: Provisioning Service

This configuration example shows only CFM-related commands. All commands that are required to set up the data path and configure the VLANs on the device are not shown. However, it should be noted that CFM traffic will not flow into or out of the device if the VLANs are not properly configured.

```
CE-A
!
ethernet cfm domain Customer level 7
service Customer1 evc evc1 vlan 100

!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2 / use an appropriate device-specific interface
ethernet cfm mep level 7 direction outward domain Customer1 mpid 701 vlan 100
!
ethernet cfm cc enable level 7 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
U-PE A
!
ethernet cfm domain Customer level 7
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
service MetroCustomer10pA evc evc1 vlan 100
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
 service MetroCustomer10pA evc evc1 vlan 100
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2  /use an appropriate device-specific interface
ethernet cfm mip level 7
ethernet cfm mep level 4 mpid 401 vlan 100
ethernet cfm mep level 1 mpid 101 vlan 100
!
interface gigabitethernet0/0/2 /use an appropriate device-specific interface
ethernet cfm mip level 1
!
ethernet cfm cc enable level 4 vlan 100
ethernet cfm cc enable level 1 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
PE-AGG A
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
service MetroCustomer10pA evc evc1 vlan 100
!
ethernet cfm global
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 1
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 1
```

```
N-PE A
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
service MetroCustomer1 evc evc1 vlan 100
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
service MetroCustomer10pA evc evc1 vlan 100
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 1
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 4
ethernet cfm mep level 1 mpid 102 vlan 100
!
ethernet cfm cc enable level 1 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
U-PE B
!
ethernet cfm domain Customer level 7
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
service MetroCustomer1 evc evc1 vlan 100
!
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
service MetroCustomer10pB evc evc1 vlan 100
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 7
ethernet cfm mep level 4 mpid 402 vlan 100
ethernet cfm mep level 2 mpid 201 vlan 100
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 2
!
ethernet cfm cc enable level 4 vlan 100
ethernet cfm cc enable level 2 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
PE-AGG B
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
service MetroCustomer10pB evc evc1 vlan 100
!
ethernet cfm global
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 2
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 2
```

```
N-PE B
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
service MetroCustomer1 evc evc1 vlan 100
!
ethernet cfm domain OperatorB level 2
mep archive-hold-time 65
service MetroCustomer10pB evc evc1 vlan 100
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 2
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mip level 4
ethernet cfm mep level 2 mpid 202 vlan 100
!
ethernet cfm cc enable level 2 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
CE-B
!
ethernet cfm domain Customer level 7
service Customer1 vlan 100
!
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet0/0/2 use an appropriate device-specific interface
ethernet cfm mep level 7 direction outward domain Customer1 mpid 702 vlan 100
!
ethernet cfm cc enable level 7 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
```

Glossary

CCM—continuity check message. A multicast CFM frame that a MEP transmits periodically to ensure continuity across the maintenance entities to which the transmitting MEP belongs, at the MA level on which the CCM is sent. No reply is sent in response to receiving a CCM.

EVC—Ethernet virtual connection. An association of two or more user-network interfaces.

fault alarm—An out-of-band signal, typically an SNMP notification, that notifies a system administrator of a connectivity failure.

inward-facing MEP—A MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the bridge relay entity.

maintenance domain—The network or part of the network belonging to a single administration for which faults in connectivity are to be managed. The boundary of a maintenance domain is defined by a set of DSAPs, each of which may become a point of connectivity to a service instance.

maintenance domain name—The unique identifier of a domain that CFM is to protect against accidental concatenation of service instances.

MEP—maintenance endpoint. An actively managed CFM entity associated with a specific DSAP of a service instance, which can generate and receive CFM frames and track any responses. It is an endpoint of a single MA, and terminates a separate maintenance entity for each of the other MEPs in the same MA.

MEP CCDB—A database, maintained by every MEP, that maintains received information about other MEPs in the maintenance domain.

MIP—maintenance intermediate point. A CFM entity, associated with a specific pair of ISS SAPs or EISS Service Access Points, which reacts and responds to CFM frames. It is associated with a single maintenance association and is an intermediate point within one or more maintenance entities.

MIP CCDB—A database of information about the MEPs in the maintenance domain. The MIP CCDB can be maintained by a MIP.

MP—maintenance point. Either a MEP or a MIP.

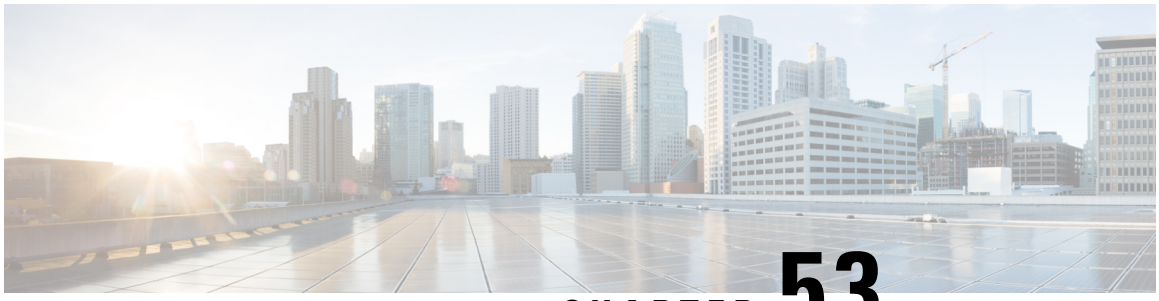
MPID—maintenance endpoint identifier. A small integer, unique over a given MA, that identifies a specific MEP.

OAM—operations, administration, and maintenance. A term used by several standards bodies to describe protocols and procedures for operating, administrating, and maintaining networks. Examples are ATM OAM and IEEE Std. 802.3ah OAM.

operator—Entity that provides a service provider a single network of provider bridges or a single Layer 2 or Layer 3 backbone network. An operator may be identical to or a part of the same organization as the service provider. For purposes of IEEE P802.1ag, Draft Standard for Local and Metropolitan Area Networks, the operator and service provider are presumed to be separate organizations.

Terms such as “customer,” “service provider,” and “operator” reflect common business relationships among organizations and individuals that use equipment implemented in accordance with IEEE P802.1ag.

UNI—user-network interface. A common term for the connection point between an operator's bridge and customer equipment. A UNI often includes a C-VLAN-aware bridge component. The term UNI is used broadly in the IEEE P802.1ag standard when the purpose for various features of CFM are explained. UNI has no normative meaning.



CHAPTER 53

Configuring Ethernet CFM for Cisco QFP-Based Platforms

IEEE Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer Operations, Administration, and Maintenance (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

This document describes the implementation of IEEE 802.1ag Standard-Compliant CFM (IEEE CFM) and Y.1731 in Cisco IOS XE software for Cisco QFP-based platforms. Y.1731 is an ITU-T recommendation for OAM functions in Ethernet-based networks. IEEE CFM and Y.1731 together will be called "Ethernet CFM" throughout this document.

Cisco QFP-based platforms inlcude ASR 1000 series routers, ISR 1000 series routers, ISR 4000 series routers, and C8000v series virtual routers.

Prerequisites for Configuring Ethernet CFM for Cisco QFP-Based Platforms

- The network topology and network administration have been evaluated.
- Business and service policies have been established.
- EVC associated with CFM domain must be configured with the L2VFI interface command
  - Before configuring CFM over L2VFI ensure EVC and Bridge Domain are configured.
  - Bridge-domain under L2VFI must be configured prior to configuring CFM MEP

Restrictions for Configuring Ethernet CFM for Cisco QFP-Based Platforms

- Ethernet CFM on Cisco QFP-based platforms is not compatible with prestandard CFM.
- Locked Signal (ETH-LCK) and Test Signal (ETH-Test) are not supported.
- Link Trace (ETH-LTM/ETH-LTR) over L2VFI is not supported.
- Initiating ETH-DMM/ETH-SLM test on MEP of EVC/EVC+VLAN MA is supported.
- Initiating ETH-DMM/ETH-SLM test on MEP of port MA is not supported.
- Configuring MIP/MEP under L2VFI is not supported.
- For Connectivity Performance Management functionalities, only single-ended delay (ETH-DM) is supported.
- QinQ encapsulation is not supported on Cisco QFP-based platforms for CFM for routed subinterfaces.
- EVPN EFI does not support association into EVC. In an EVPN scenario, it only supports configuring down MEP on the EFP. Up MEP cannot send CFM packet out from the EFI to the peer site.
- Cisco private CFM protocol is not supported. IEEE standard CFM protocol is supported.

Information About Configuring Ethernet CFM for Cisco QFP-Based Platforms

Ethernet CFM

IEEE CFM is an end-to-end per-service Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End to end can be provider edge to provider edge (PE to PE) or customer edge to customer edge (CE to CE).

Ethernet CFM is distinct from other metro-Ethernet OAM protocols by being an end-to-end technology. For example, Multiprotocol Label Switching (MPLS), ATM, and SONET OAM help in debugging Ethernet wires but are not always end to end. 802.3ah OAM is a single-hop and per-physical-wire protocol. It is not end to end or service aware. Ethernet Local Management Interface (E-LMI) is confined between the user-end provider edge (uPE) and CE and relies on CFM for reporting status of the metro-Ethernet network to the CE.

The benefits of Ethernet CFM are:

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers

Benefits of Ethernet CFM

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers

Maintenance Associations

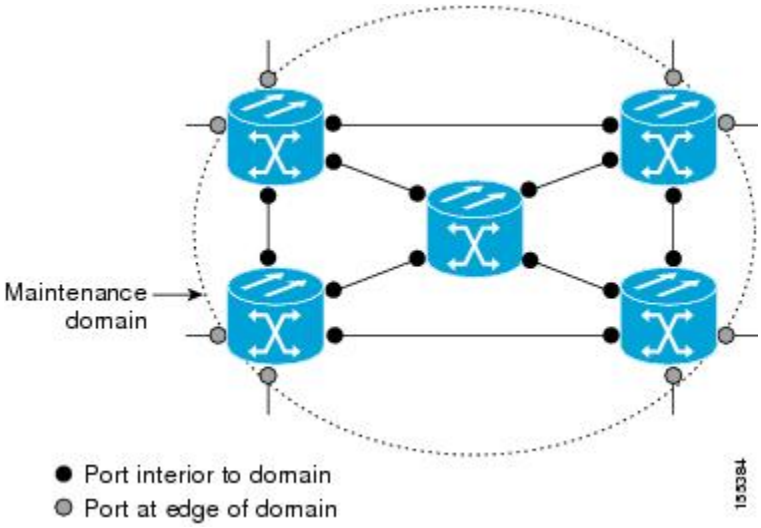
An MA identifies a service that can be uniquely identified within a maintenance domain. There can be many MAs within a domain. The MA direction is specified when the MA is configured. The short MA name must be configured on a domain before MEPs can be configured.

The CFM protocol runs for a specific MA.

Maintenance Domains

A maintenance domain is a management space for the purpose of managing and administering a network. A domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary. The figure below illustrates a typical maintenance domain.

Figure 35: A Typical Maintenance Domain



A unique maintenance level in the range of 0 to 7 is assigned to each domain by a network administrator. Levels and domain names are useful for defining the hierarchical relationship among domains. The hierarchical relationship of domains parallels that of customer, service provider, and operator. The larger the domain, the higher the level value. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators would have the smallest domains and customers the largest domains, with service provider domains between them in size. All levels of the hierarchy must operate together.

Domains should not intersect because intersecting would mean management by more than one entity, which is not allowed. Domains may nest or touch but when two domains nest, the outer domain must have a higher maintenance level than the domain nested within it. Nesting maintenance domains is useful in the business

model where a service provider contracts with one or more operators to provide Ethernet service to a customer. Each operator would have its own maintenance domain and the service provider would define its domain--a superset of the operator domains. Furthermore, the customer has its own end-to-end domain, which is in turn a superset of the service provider domain. Maintenance levels of various nesting domains should be communicated among the administering organizations. For example, one management approach would be to have the service provider assign maintenance levels to operators.

Ethernet CFM exchanges messages and performs operations on a per-domain basis. For example, running CFM at the operator level does not allow discovery of the network by the higher provider and customer levels.

Network designers determine domain configurations.

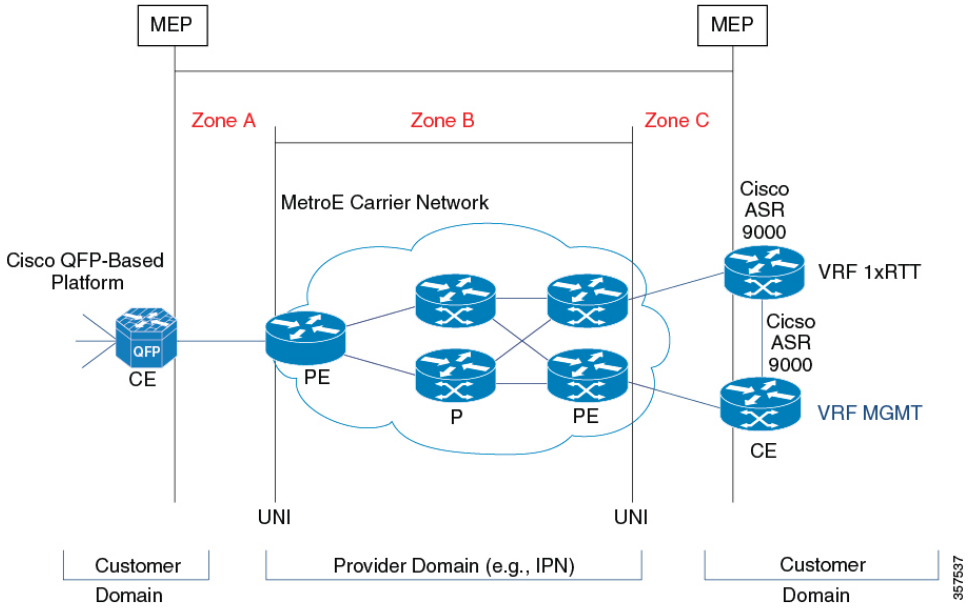
The following characteristics of domains are supported:

- Name is a maximum of 154 characters in length.
- Direction is specified when the MA is configured.
- Down (toward the wire) MEPs.

A domain can be removed when all maintenance points within the domain have been removed and all remote MEP entries in the continuity check database (CCDB) for the domain have been purged.

The figure below illustrates service provider and customer domains and where the Cisco QFP-based platform is in the network.

Figure 36: Service Provider and Customer Domains



Maintenance Points

A maintenance point (MIP) is a demarcation point on an interface or port that participates in Connectivity Fault Management (CFM) within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. Two classes of maintenance points exist, maintenance end points (MEPs) and MIPs. Support for MIPs varies by Cisco release.

Maintenance Association Endpoints

Maintenance association endpoints (MEPs) reside at the edge of a maintenance domain and confine Ethernet Connectivity Fault Management (CFM) messages within the domain via the maintenance domain level. MEPs periodically transmit and receive continuity check messages (CCMs) from other MEPs within the domain. At the request of an administrator, linktrace and loopback messages can also be transmitted. MEPs are either "Up" (toward the bridge) or "Down" (toward the wire). Support for Up MEPs varies by Cisco release.

When the **continuity-check static rmep** command is configured on a port MEP and continuity checking does not detect a removed MEP, the port is set to MAC operation down and the interface protocol is set to down. Normal traffic is stopped because the line protocol is down, but CFM packets still pass.

MEP configurations can be removed after all pending loopback and traceroute replies are removed and the service on the interface is set to transparent mode.

Down MEPs for Routed Ports

Down MEPs communicate through the wire.

Down MEPs use the port MAC address.

A Down MEP performs the following functions:

- Sends and receives Ethernet CFM frames at its level via the wire connected to the port where the MEP is configured.
- Processes all Ethernet CFM frames at its level coming from the direction of the wire.
- Drops all Ethernet CFM frames at a lower level coming from the direction of the wire.
- Transparently drops all Ethernet CFM frames at a higher level, independent of whether they came in from the bridge or wire.

Ethernet CFM Messages

Ethernet CFM uses standard Ethernet frames. Ethernet CFM frames are distinguishable by EtherType and for multicast messages by MAC address. Ethernet CFM frames are sourced, terminated, processed, and relayed by bridges. Routers can support only limited Ethernet CFM functions.

Bridges that cannot interpret Ethernet CFM messages forward them as normal data frames. All Ethernet CFM messages are confined to a maintenance domain and to an MA. Three types of messages are supported:

- Continuity Check
- Linktrace
- Loopback

Continuity Check Messages

Ethernet CFM continuity check messages (CCMs) are multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain. CCMs are confined to a domain.

CFM CCMs have the following characteristics:

- Transmitted at a periodic interval by MEPs. The minimum interval is 3.3 milliseconds (ms).

- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Indicate the status of the interface on which the MEP is configured.

Linktrace Messages

Ethernet CFM linktrace messages (LTMs) are multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They are similar to Layer 3 traceroute messages. LTMs allow the transmitting node to discover vital connectivity data about the path. LTMs are intercepted by maintenance points along the path and processed, transmitted, or dropped. At each hop where there is a maintenance point at the same level, a linktrace message reply (LTR) is transmitted back to the originating MEP. For each visible MIP, linktrace messages indicate ingress action, relay action, and egress action.

Linktrace messages include the destination MAC address, VLAN, and maintenance domain and they have Time To Live (TTL) to limit propagation within the network. They can be generated on demand using the CLI. LTMs are multicast and LTRs are unicast.

Loopback Messages

Ethernet CFM loopback messages (LBMs) are unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message (LBR) indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.

Because LBMs are unicast, they are forwarded like normal data frames except with the maintenance level restriction. If the outgoing port is known in the bridge's forwarding database and allows Ethernet CFM frames at the message's maintenance level to pass through, the frame is sent out on that port. If the outgoing port is unknown, the message is broadcast on all ports in that domain.

An Ethernet CFM LBM can be generated on demand using the CLI. The source of a loopback message must be a MEP. Both Ethernet CFM LBMs and LBRs are unicast, and LBMs specify the destination MAC address or MEP identifier (MPID), VLAN, and maintenance domain.

Cross-Check Function

The cross-check function is a timer-driven postprovisioning service verification between dynamically discovered MEPs (via continuity check messages CCMs)) and expected MEPs (via configuration) for a service. The cross-check function verifies that all endpoints of a multipoint or point-to-point service are operational. The function supports notifications when the service is operational; otherwise it provides alarms and notifications for unexpected or missing endpoints.

The cross-check function is performed one time. You must initiate the cross-check function from the CLI every time you want a service verification.

SNMP Traps

The support provided by the Cisco IOS XE software implementation of Ethernet CFM traps is Cisco proprietary information. MEPs generate two types of Simple Network Management Protocol (SNMP) traps, continuity check (CC) traps and cross-check traps.

CC Traps

- MEP up--Sent when a new MEP is discovered, the status of a remote port changes, or connectivity from a previously discovered MEP is restored after interruption.
- MEP down--Sent when a timeout or last gasp event occurs.
- Cross-connect--Sent when a service ID does not match the VLAN.
- Loop--Sent when a MEP receives its own CCMs.
- Configuration error--Sent when a MEP receives a continuity check with an overlapping MPID.

Cross-Check Traps

- Service up--Sent when all expected remote MEPs are up in time.
- MEP missing--Sent when an expected MEP is down.
- Unknown MEP--Sent when a CCM is received from an unexpected MEP.

Steps to Generate SNMP Traps for CFM

To generate SNMP traps, following commands need to be configured on the router.

```
ethernet cfm logging
logging snmp-trap 0 7
logging history debugging
```

Send Trap to SNMP Server

```
snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]
snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [ service-up]
```

Note If syslog trap is enabled, by default trap is generated for messages of severity level emergency, alert, critical, error and warning (0-4). For other severity levels need to enable **logging snmp-trap 0 7** and **logging history debugging**

```
Router(config)#ethernet cfm logging
Router(config)#logging snmp-trap 0 7
Router(config)#logging history debugging
Router(config)#snmp-server enable traps ethernet cfm cc
Router(config)#snmp-server enable traps ethernet cfm crosscheck
```

Logs for MEP going DOWN

```
Console-logs:

Router(config)#
*Oct 26 21:32:06.663 IST: %E_CFM-3-REMOTE_MEP_DOWN: Remote MEP mpid 10 evc 2 vlan 2 MA name
 s2 in domain cust2 changed state to down with event code TimeOut.
*Oct 26 21:32:06.664 IST: %E_CFM-6-ENTER_AIS: local mep with mpid 20 level 2 BD/VLAN 2 dir
 D Interface Te0/3/1 enters AIS defect condition
*Oct 26 21:32:09.147 IST: %E_CFM-3-FAULT_ALARM: A fault has occurred in the network for the
```

```
 local MEP having mpid 20 evc 2 vlan 2 for service MA name s2 with the event code
DefRemoteCCM.
```

SNMP Server Side Logs

Received SNMPv2c Trap

```
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:00:54.27
snmpTrapOID.0 = clogMessageGenerated
clogHistFacility.76 = E_CFM
clogHistSeverity.76 = error(4)
clogHistMsgName.76 = REMOTE_MEP_DOWN
clogHistMsgText.76 = Remote MEP mpid 10 evc 2 vlan 2 MA name s2 in domain cust2 changed
state to down with event code TimeOut.
clogHistTimestamp.76 = 04:00:54.27
```

Received SNMPv2c Trap

```
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:00:54.27
snmpTrapOID.0 = clogMessageGenerated
clogHistFacility.77 = E_CFM
clogHistSeverity.77 = info(7)
clogHistMsgName.77 = ENTER_AIS
clogHistMsgText.77 = local mep with mpid 20 level 2 BD/VLAN 2 dir D Interface Te0/3/1 enters
 AIS defect condition
clogHistTimestamp.77 = 04:00:54.27
```

Received SNMPv2c Trap

```
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:00:56.75
snmpTrapOID.0 = dot1agCfmFaultAlarm
dot1agCfmMepHighestPrDefect.10.2.20 = defRemoteCCM(3)
```

Received SNMPv2c Trap

```
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:00:56.75
snmpTrapOID.0 = clogMessageGenerated
clogHistFacility.78 = E_CFM
clogHistSeverity.78 = error(4)
clogHistMsgName.78 = FAULT_ALARM
clogHistMsgText.78 = A fault has occurred in the network for the local MEP having mpid 20
evc 2 vlan 2 for service MA name s2 with the event code DefRemoteCCM.
clogHistTimestamp.78 = 04:00:56.75
```

Logs for MEP Coming Up

Console-logs

```
================================================
Router(config)#
*Oct 26 21:35:03.780 IST: %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from
 a remote MEP with mpid 10 evc 2 vlan 2 MA name s2 domain cust2 interface status Up event
code Returning.
*Oct 26 21:35:03.781 IST: %E_CFM-6-EXIT_AIS: local mep with mpid 20 level 2 BD/VLAN 2 dir
D Interface Te0/3/1 exited AIS defect condition
```

SNMP Server Side Logs

Received SNMPv2c Trap

```
================================================
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:03:51.39
snmpTrapOID.0 = clogMessageGenerated
clogHistFacility.79 = E_CFM
clogHistSeverity.79 = info(7)
clogHistMsgName.79 = REMOTE_MEP_UP
clogHistMsgText.79 = Continuity Check message is received from a remote MEP with mpid 10
evc 2 vlan 2 MA name s2 domain cust2 interface status Up event code Returning.
clogHistTimestamp.79 = 04:03:51.38
```

Received SNMPv2c Trap

```
Community: public
From: 7.32.22.154
sysUpTimeInstance = 04:03:51.39
snmpTrapOID.0 = clogMessageGenerated
clogHistFacility.80 = E_CFM
clogHistSeverity.80 = info(7)
clogHistMsgName.80 = EXIT_AIS
clogHistMsgText.80 = local mep with mpid 20 level 2 BD/VLAN 2 dir D Interface Te0/3/1 exited
 AIS defect condition
clogHistTimestamp.80 = 04:03:51.38
```

HA Feature Support in Ethernet CFM

In access and service provider networks using Ethernet technology, High availability (HA) is a requirement. End-to-end connectivity status information is critical and must be maintained on a hot standby Route Processor (RP).

Note A hot standby RP has the same software image as the active RP and supports synchronization of line card, protocol, and application state information between RPs for supported features and protocols.

End-to-end connectivity status is maintained on the CE, PE, and access aggregation PE (uPE) network nodes based on information received by protocols such as Ethernet local management interface (LMI) and CFM, and 802.3ah. This status information is used to either stop traffic or switch to backup paths when an interface is down.

Every transaction involves either accessing or updating data among various databases. If the database is synchronized across active and standby modules, the modules are transparent to clients.

The Cisco infrastructure provides various component application program interfaces (APIs) that help to maintain a hot standby RP. Metro Ethernet HA clients CFM HA and in-service software upgrades (ISSU) interact with these components, update the database, and trigger necessary events to other components.

Benefits of CFM HA

- Elimination of network downtime for Cisco software image upgrades, allowing for faster upgrades that result in high availability.
- Elimination of resource scheduling challenges associated with planned outages and late night maintenance windows.
- Accelerated deployment of new services and applications and facilitation of faster implementation of new features, hardware, and fixes than if HA was not supported.
- Reduced operating costs due to outages while delivering high service levels.
- CFM updates its databases and controls its own HA messaging and versioning, and this control facilitates maintenance.

NSF SSO Support in Ethernet CFM

The redundancy configurations SSO and NSF are both supported in Ethernet CFM and are automatically enabled. A switchover from an active to a standby RP occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance. NSF interoperates with the SSO feature to minimize network downtime following a switchover. The primary function of Cisco NSF is to continue forwarding packets following an RP switchover.

For detailed information about SSO, see the “Stateful Switchover” module of the *Cisco IOS High Availability Configuration Guide*. For detailed information about the NSF feature, see the “Cisco Nonstop Forwarding” module of the *High Availability Configuration Guide*.

ISSU Support in Ethernet CFM

In Service Upgrades (ISSU) allows you to perform a Cisco software upgrade or downgrade without disrupting packet flow. Ethernet Connectivity Fault Management (CFM) performs a bulk update and a runtime update of the continuity check database to the standby route processor (RP), including adding, deleting, or updating a row. This checkpoint data requires ISSU capability to transform messages from one release to another. All the components that perform active RP to standby RP updates using messages require ISSU support.

ISSU is automatically enabled in Ethernet CFM and lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. For detailed information about ISSU, see the “Cisco IOS In Service Software Upgrade Process” module of the *High Availability Configuration Guide*.

How to Configure Ethernet CFM for Cisco QFP-Based Platforms

Designing CFM Domains

Note To have an operator, service provider, or customer domain is optional. A network may have a single domain or multiple domains. The steps listed here show the sequence when all three types of domains will be assigned.

Before you begin

- Knowledge and understanding of the network topology.
- Understanding of organizational entities involved in managing the network; for example, operators, service providers, network operations centers (NOCs), and customer service centers.
- Understanding of the type and scale of services to be offered.
- Agreement by all organizational entities on the responsibilities, roles, and restrictions for each organizational entity.
- Determination of the number of maintenance domains in the network.
- Determination of the nesting and disjoint maintenance domains.
- Assignment of maintenance levels and names to domains based on agreement between the service provider and operator or operators.
- Determination of whether the domain should be inward or outward.

SUMMARY STEPS

1. Determine operator level MIPs.
2. Determine operator level MEPs.
3. Determine service provider MIPs.
4. Determine service provider MEPs.
5. Determine customer MIPs.
6. Determine customer MEPs.

DETAILED STEPS

Step 1 Determine operator level MIPs.

Follow these steps:

- Starting at lowest operator level domain, assign a MIP at every interface internal to the operator network to be visible to CFM.
- Proceed to next higher operator level and assign MIPs.

- Verify that every port that has a MIP at a lower level does not have maintenance points at a higher level.
- Repeat steps a through d until all operator MIPs are determined.

Step 2 Determine operator level MEPs.

Follow these steps:

- Starting at the lowest operator level domain, assign a MEP at every UNI that is part of a service instance.
- Assign a MEP at the network to network interface (NNI) between operators, if there is more than one operator.
- Proceed to next higher operator level and assign MEPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should have either a MIP or MEP at a higher level.

Step 3 Determine service provider MIPs.

Follow these steps:

- Starting at the lowest service provider level domain, assign service provider MIPs at the NNI between operators (if more than one).
- Proceed to next higher service provider level and assign MIPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should not have either a MIP or a MEP at a higher level.

Step 4 Determine service provider MEPs.

Follow these steps:

- Starting at the lowest service provider level domain, assign a MEP at every UNI that is part of a service instance.
- Proceed to next higher service provider level and assign MEPs.
- A port with a MIP at a lower level cannot have maintenance points at a higher level. A port with a MEP at a lower level should have either a MIP or a MEP at a higher level.

Step 5 Determine customer MIPs.

Customer MIPs are allowed only on the UNIs at the uPEs if the service provider allows the customer to run CFM. Otherwise, the service provider can configure Cisco devices to block CFM frames.

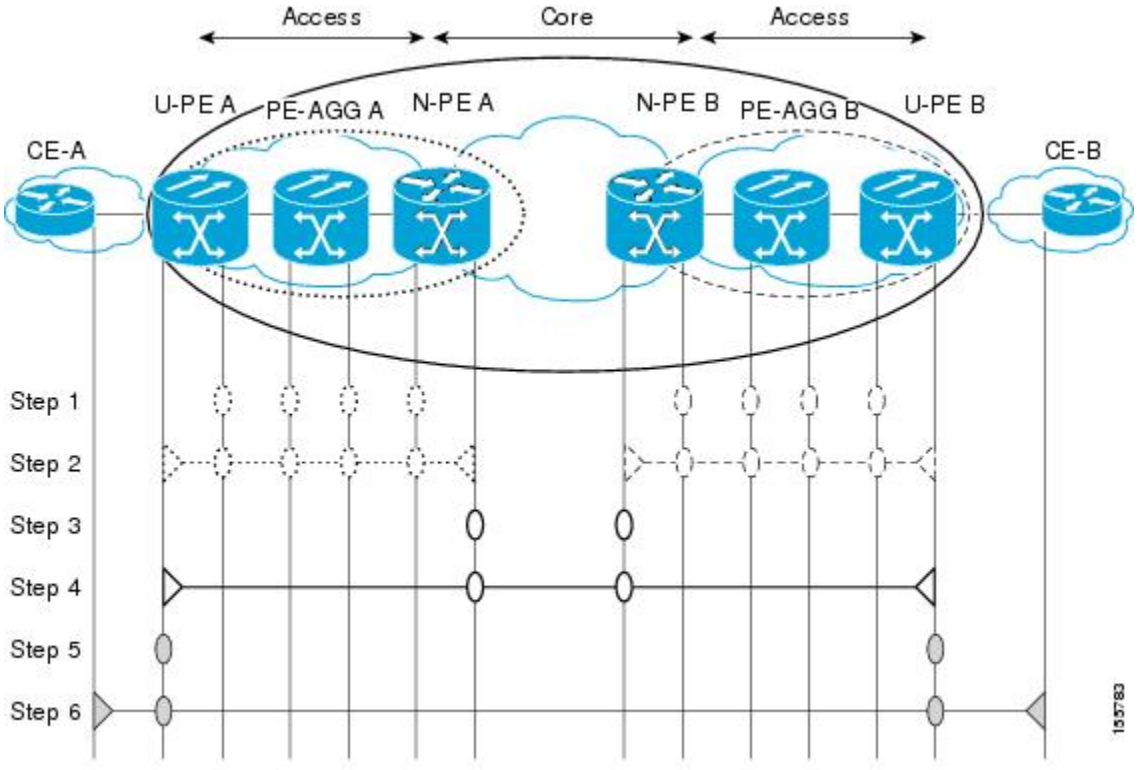
- Configure a MIP on every uPE, at the UNI port, in the customer maintenance domain.
- Ensure the MIPs are at a maintenance level that is at least one higher than the highest level service provider domain.

Step 6 Determine customer MEPs.

Customer MEPs are on customer equipment. Assign an outward facing MEP within an outward domain at the appropriate customer level at the handoff between the service provider and the customer.

Examples

The figure below shows an example of a network with a service provider and two operators, A and B. Three domains are to be established to map to each operator and the service provider. In this example, for simplicity we assume that the network uses Ethernet transport end to end. CFM, however, can be used with other transports.



Configuring Ethernet CFM

Provisioning the Network (CE-A)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **mep archive-hold-time** *minutes*
5. **exit**
6. **ethernet cfm global**
7. **ethernet cfm ieee**
8. **ethernet cfm traceroute cache**
9. **ethernet cfm traceroute cache size** *entries*
10. **ethernet cfm traceroute cache hold-time** *minutes*

11. **ethernet cfm logging** [**alarm ieee** | **cisco**] [**ais**]
12. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
13. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**]
14. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 5	**exit** **Example:** `Device(config-ecfm)# exit`	Returns the device to global configuration mode.
Step 6	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 7	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the CFM IEEE version of CFM. • This command is automatically issued when the **ethernet cfm global** command is issued.
Step 8	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.

	Command or Action	Purpose
Step 9	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 10	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 11	**ethernet cfm logging** [**alarm ieee** | **cisco**] [**ais**] **Example:** `Device(config)#ethernet cfm logging`	Enables generating CFM syslog messages.
Step 12	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM continuity check events.
Step 13	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown`	Enables SNMP trap generation for Ethernet CFM continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 14	**end** **Example:** `Device(config)# end`	Returns the device to privileged EXEC mode.

Provisioning the Network (CE-B)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **mep archive-hold-time** *minutes*
5. **exit**
6. **ethernet cfm global**
7. **ethernet cfm ieee**

8. **ethernet cfm traceroute cache**
9. **ethernet cfm traceroute cache size** *entries*
10. **ethernet cfm traceroute cache hold-time** *minutes*
11. **ethernet cfm logging** [**alarm ieee** | **cisco**] [**ais**]
12. **snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**]
13. **snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**]
14. **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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines an outward CFM maintenance domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 5	**exit** **Example:** `Device(config-ecfm)# exit` **Example:**	Returns the device to global configuration mode.
Step 6	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 7	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the CFM IEEE version of CFM. • This command is automatically issued when the **ethernet cfm global** command is issued.

	Command or Action	Purpose
Step 8	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 9	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 10	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 11	**ethernet cfm logging** [**alarm ieee** | **cisco**] [**ais**] **Example:** `Device(config)#ethernet cfm logging`	Enables generating CFM syslog messages.
Step 12	**snmp-server enable traps ethernet cfm cc** [**mep-up**] [**mep-down**] [**config**] [**loop**] [**cross-connect**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop cross-connect`	Enables SNMP trap generation for Ethernet CFM mep-up, mep-down, config, loop, and cross-connect events.
Step 13	**snmp-server enable traps ethernet cfm crosscheck** [**mep-unknown**] [**mep-missing**] [**service-up**] **Example:** `Device(config)# snmp-server enable traps ethernet cfm crosscheck mep-unknown`	Enables SNMP trap generation for Ethernet CFM mep-unknown, mep-missing, and service-up continuity check events in relation to the cross-check operation between statically configured MEPs and those learned via CCMs.
Step 14	**end** **Example:** `Device(config)# end` **Example:**	Returns the device to privileged EXEC mode.

Provisioning Service (CE-A)

Perform this task to set up service for Ethernet CFM. Optionally, when this task is completed, you may configure and enable the cross-check function. To perform this optional task, see "Configuring and Enabling the Cross-Check Function (CE-A)".

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **evc***evc-name*[**vlan** *vlan-id*] [**direction down**]]
5. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
6. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
7. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
8. **exit**
9. **mep archive-hold-time** *minutes <1-65535>*
10. **exit**
11. **ethernet cfm global**
12. **ethernet cfm ieee**
13. **ethernet cfm traceroute cache**
14. **ethernet cfm traceroute cache size** *entries*
15. **ethernet cfm traceroute cache hold-time** *minutes*
16. **interface** *type number*
17. **ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id* | **service***service-name*}
18. **end**
19. **interface***interface-name* **encapsulation dot1q** *vlan-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Router(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a specified maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **evc***evc-name*[**vlan** *vlan-id*] [**direction down**]] **Example:**	Configures an MA within a maintenance domain and enters CFM service configuration mode. • If a service is already configured and you configure a new MA name and also specify the **direction down** keyword, a second service is added that maps to the

	Command or Action	Purpose
	`Router(config-ecfm)# service Customer1 evc EVC1 vlan 100 direction down`	same VLAN. If you configure a new MA name and do not specify the **direction down** keyword, the service is renamed to the new MA name. • If direction down is not specified, then the default value is direction up. Router port only supports configuring MEP in direction down MA.
Step 5	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Router(config-ecfm-srv)# continuity-check`	Enables the transmission of CCMs.
Step 6	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Router(config-ecfm-srv)# continuity-check interval 10s`	Configures the time period between CCM transmissions. • The values supported are platform dependent. • QFP-based platforms support intervals of 3.3ms/ 10ms/ 100ms/ 1s/ 10s/ 1m/ 10m. The default CCM interval is 10s.
Step 7	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Router(config-ecfm-srv)# continuity-check loss-threshold 10`	Sets the number of CCMs that should be missed before declaring that a remote MEP is down. The default loss-threshold is 3.
Step 8	**exit** **Example:** `Router(config-ecfm-srv)# exit` **Example:**	Returns the device to Ethernet CFM configuration mode.
Step 9	**mep archive-hold-time** *minutes <1-65535>* **Example:** `Router(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged. The default hold time is 100 minutes.
Step 10	**exit** **Example:** `Router(config-ecfm)# exit`	Returns the device to global configuration mode.
Step 11	**ethernet cfm global** **Example:** `Router(config)# ethernet cfm global`	Enables CFM processing globally on the device.

	Command or Action	Purpose
Step 12	**ethernet cfm ieee** **Example:** `Router(config)# ethernet cfm ieee`	Enables the CFM IEEE version of CFM. • This command is automatically issued when the **ethernet cfm global** command is issued.
Step 13	**ethernet cfm traceroute cache** **Example:** `Router(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 14	**ethernet cfm traceroute cache size** *entries* **Example:** `Router(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 15	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Router(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 16	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/3`	Specifies an interface and enters interface configuration mode.

Step 17	**ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id* | **service***service-name*}
	Example:
	`Router(config-if)# ethernet cfm mep domain Customer mpid 701 vlan 100`
	or
	`Router(config-if)# ethernet cfm mep domain Customer mpid 701 service Customer1`
		Sets a port as internal to a maintenance domain and defines it as a MEP.
		The VLAN 100 or the service Customer1 can point to the same MA.

Step 18	**end** **Example:** `Router(config-if)# end`	Returns the device to privileged EXEC mode.

Step 19	**interface***interface-name* **encapsulation dot1q** *vlan-id*
	Example:
	`Router(config)#interface ethernet0/3.100`
	`Router(config-subif)#encapsulation dot1Q 100`
		Creates sub-interface with the VLAN 100 of the specific MA.

Provisioning Service (CE-B)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **mep archive-hold-time** *minutes*
5. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **evc***evc-name* [**vlan** *vlan-id*] [**direction down**]]
6. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
7. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
8. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
9. **exit**
10. **exit**
11. **ethernet cfm global**
12. **ethernet cfm ieee**
13. **ethernet cfm traceroute cache**
14. **ethernet cfm traceroute cache size** *entries*
15. **ethernet cfm traceroute cache hold-time** *minutes*
16. **interface** *slot*/*subslot*/*port*
17. **ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id* | **service** *service-name*}
18. **end**
19. **interface** *interface-name* **encapsulation dot1q** *vlan-id*

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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM maintenance domain at a specified level and enters Ethernet CFM configuration mode.

	Command or Action	Purpose
Step 4	**mep archive-hold-time** *minutes* **Example:** `Device(config-ecfm)# mep archive-hold-time 60`	Sets the amount of time that data from a missing MEP is kept in the continuity check database or that entries are held in the error database before they are purged.
Step 5	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **evc***evc-name* [**vlan** *vlan-id*] [**direction down**]] **Example:** `Device(config-ecfm)# service Customer1 evc EVC1 vlan 100 direction down`	Configures an MA within a maintenance domain and enters CFM service configuration mode. • If a service is already configured and you configure a new MA name and also specify the **direction down** keyword, a second service is added that maps to the same VLAN. If you configure a new MA name and do not specify the **direction down** keyword, the service is renamed to the new MA name. • If direction down is not specified, then the default value is direction up. Router port only supports configuring MEP in direction down MA.
Step 6	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Device(config-ecfm-srv)# continuity-check`	Enables the transmission of CCMs.
Step 7	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Device(config-ecfm-srv)# continuity-check interval 10s`	Configures the time period between CCM transmissions. • The values supported are platform dependent. • QFP-based platforms support intervals of 3.3ms/ 10ms/ 100ms/ 1s/ 10s/ 1m/ 10m. The default CCM interval is 10s.
Step 8	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Device(config-ecfm-srv)# continuity-check loss-threshold 10`	Sets the number of CCMs that should be missed before declaring that a remote MEP is down. The default loss-threshold is 3.
Step 9	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns the device to Ethernet CFM configuration mode.
Step 10	**exit** **Example:** `Device(config-ecfm)# exit`	Returns the device to global configuration mode.

	Command or Action	Purpose
Step 11	**ethernet cfm global** **Example:** `Device(config)# ethernet cfm global`	Enables CFM processing globally on the device.
Step 12	**ethernet cfm ieee** **Example:** `Device(config)# ethernet cfm ieee`	Enables the CFM IEEE version of CFM. • This command is automatically issued when the **ethernet cfm global** command is issued.
Step 13	**ethernet cfm traceroute cache** **Example:** `Device(config)# ethernet cfm traceroute cache`	Enables caching of CFM data learned through traceroute messages.
Step 14	**ethernet cfm traceroute cache size** *entries* **Example:** `Device(config)# ethernet cfm traceroute cache size 200`	Sets the maximum size for the CFM traceroute cache table.
Step 15	**ethernet cfm traceroute cache hold-time** *minutes* **Example:** `Device(config)# ethernet cfm traceroute cache hold-time 60`	Sets the amount of time that CFM traceroute cache entries are retained.
Step 16	**interface** *slot/subslot/port* **Example:** `Device(config)# interface ethernet 0/3`	Specifies an interface and enters interface configuration mode.

Step 17	**ethernet cfm mep domain** *domain-name* **mpid** *mpid* {**port** | **vlan** *vlan-id* | **service** *service-name*}
	Example:
	`Device(config-if)# ethernet cfm mep domain Customer mpid 702 vlan 100`
	or
	`Device(config-if)# ethernet cfm mep domain Customer mpid 702 service Customer1`
		Provisions an interface as a domain boundary.
		The VLAN 100 or the service Customer1 can point to the same MA.

Step 18	**end** **Example:** `Device(config-if)# end`	Returns the device to privileged EXEC mode.

	Command or Action	Purpose

Step 19	**interface** *interface-name* **encapsulation dot1q** *vlan-id*
	Example:
	`Router(config)#interface ethernet0/3.100`
	`Router(config-subif)#encapsulation dot1Q 100`
		Creates sub-interface with the VLAN 100 of the specific MA.

Configuring and Enabling the Cross-Check Function (CE-A)

Perform this task to configure and enable cross-checking for a down MEP. This task requires you to configure and enable cross-checking on two devices. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **mep mpid** *mpid*
6. **exit**
7. **ethernet cfm mep crosscheck start-delay** *delay*
8. **exit**

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	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines a CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.

	Command or Action	Purpose
Step 5	**mep mpid** *mpid* **Example:** `Device(config-ecfm)# mep mpid 701`	Statically defines the MEPs within a maintenance association.
Step 6	**exit** **Example:** `Device(config-ecfm)# exit`	Returns the device to global configuration mode.
Step 7	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns the device to privileged EXEC mode.

Configuring and Enabling the Cross-Check Function (CE-B)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down**
5. **mep mpid** *mpid*
6. **exit**
7. **ethernet cfm mep crosscheck start-delay** *delay*
8. **exit**

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.

	Command or Action	Purpose
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* **Example:** `Device(config)# ethernet cfm domain Customer level 7`	Defines an outward CFM domain at a specified level and enters Ethernet CFM configuration mode.
Step 4	**service** *short-ma-name* **evc** *evc-name* **vlan** *vlanid* **direction down** **Example:** `Device(config-ecfm)# service s41 evc 41 vlan 41 direction down`	Configures a maintenance association within a maintenance domain and enters Ethernet connectivity fault management (CFM) service configuration mode.
Step 5	**mep mpid** *mpid* **Example:** `Device(config-ecfm)# mep mpid 702`	Statically defines the MEPs within a maintenance association.
Step 6	**exit** **Example:** `Device(config-ecfm)# exit`	Returns the device to global configuration mode.
Step 7	**ethernet cfm mep crosscheck start-delay** *delay* **Example:** `Device(config)# ethernet cfm mep crosscheck start-delay 60`	Configures the maximum amount of time that the device waits for remote MEPs to come up before the cross-check operation is started.
Step 8	**exit** **Example:** `Device(config)# exit`	Returns the device to privileged EXEC mode.

Configuring Interfaces

Configuring CFM on Physical Port

Cisco QFP-based platforms support configuring CFM on physical port.

Configuring CFM on EVC

Cisco QFP-based platforms support configuring CFM on EVC.

Configuring CFM on Sub-Interface

Cisco QFP-based platforms do not support directly configuring CFM on sub-interfaces. To deploy CFM on sub-interface, perform the following steps:

- configure EVC + VLAN MA

- configure MEP on physical interface under this EVC + VLAN MA
- configure VLAN encapsulation under sub-interface

Configuration Examples for Configuring Ethernet CFM for Cisco QFP-based Platforms

The following examples show configurations for a network. Configurations are shown not only for the Carrier Ethernet QFP-based platforms, but also for the devices used at the access and core of the service provider's network.

Example: Provisioning a Network

This configuration example shows only CFM-related commands. All commands that are required to set up the data path and configure the VLANs on the device are not shown. However, it should be noted that CFM traffic will not flow into or out of the device if the VLANs are not properly configured.

CE-A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm mip auto-create level 7 vlan 1-4094
!
interface
 ethernet cfm mip level 7 vlan 101   <<<< Manual MIP
 ethernet cfm mep domain ServiceProvider-L4 mpid 401 vlan 101
 ethernet cfm mep domain OperatorA-L1 mpid 101 vlan 101
!
interface
 ethernet cfm mip level 1 vlan 101   <<<< Manual MIP
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

U-PE A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm mip auto-create level 7 vlan 1-4094
!
interface
 ethernet cfm mip level 7 vlan 101   <<<< Manual MIP
 ethernet cfm mep domain ServiceProvider-L4 mpid 401 vlan 101
```

```
 ethernet cfm mep domain OperatorA-L1 mpid 101 vlan 101
!
interface
 ethernet cfm mip level 1 vlan 101   <<<< Manual MIP
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

PE-AGG A Configuration

```
ethernet cfm global
ethernet cfm ieee
ethernet cfm domain OperatorA-L1 level 1
mep archive-hold-time 65
  mip auto-create
  service MetroCustomer1OpA vlan 101
!
interface
 ethernet cfm mip level 1 vlan 101   <<<< Manual MIP
!
interface
 ethernet cfm mip level 1    <<<< Manual MIP
```

N-PE A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain ServiceProvider-L4 level 4
 mep archive-hold-time 60
 mip auto-create
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
 mip auto-create
service MetroCustomer1OpA vlan 101
  continuity-check
!
interface
 ethernet cfm mip level 1    <<<< manual MIP
!
interface
 ethernet cfm mip level 4    <<<< manual MIP
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

U-PE B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
```

```
ethernet cfm domain Customer-L7 level 7
 mip auto-create
 service Customer1 vlan 101 direction down
!
ethernet cfm domain ServiceProvider-L4 level 4
 mep archive-hold-time 60
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorB level 2
 mip auto-create
 mep archive-hold-time 65
 service MetroCustomer1OpB vlan 101
  continuity-check
!
interface
 ethernet cfm mip level 7   <<<< manual MIP
!
interface
 ethernet cfm mip level 2   <<<< manual MIP
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

PE-AGG B Configuration

```
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm domain OperatorB level 2
 mep archive-hold-time 65
 mip auto-create
 service MetroCustomer1OpB vlan 101
!
interface
 ethernet cfm mip level 2   <<<< manual MIP
!
interface
 ethernet cfm mip level 2   <<<< manual MIP
```

N-PE B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain ServiceProvider level 4
 mep archive-hold-time 60
 mip auto-create
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorB level 2
 mep archive-hold-time 65
 mip auto-create
 service MetroCustomer1OpB vlan 101
  continuity-check
!
interface
```

```
ethernet cfm mip level 2    <<<< manual MIP
!
interface
 ethernet cfm mip level 4   <<<< manual MIP
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

CE-B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain Customer-L7 level 7
 service Customer1 vlan 101 direction down
  continuity-check
!
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
```

Example: Provisioning Service

CE-A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain Customer-L7 level 7
 service Customer1 vlan 101 direction down
  continuity-check
!
interface
 ethernet cfm mep domain Customer-L7 mpid 701 vlan 101
```

U-PE A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm mip auto-create level 7 vlan 1-4094
!
ethernet cfm domain ServiceProvider-L4 level 4
 mep archive-hold-time 60
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorA-L1 level 1
 mep archive-hold-time 65
 mip auto-create
```

```
 service MetroCustomer1OpA vlan 101
  continuity-check
!
interface
 ethernet cfm mip level 7 vlan 101   <<<< Manual MIP
 ethernet cfm mep domain ServiceProvider-L4 mpid 401 vlan 101
 ethernet cfm mep domain OperatorA-L1 mpid 101 vlan 101
!
interface
 ethernet cfm mip level 1 vlan 101   <<<< Manual MIP
```

PE-AGG A Configuration

```
ethernet cfm global
ethernet cfm ieee
ethernet cfm domain OperatorA-L1 level 1
mep archive-hold-time 65
  mip auto-create
  service MetroCustomer1OpA vlan 101
!
interface
 ethernet cfm mip level 1 vlan 101   <<<< Manual MIP
!
interface
 ethernet cfm mip level 1    <<<< Manual MIP
```

N-PE A Configuration

```
!
ethernet cfm global
ethernet cfm ieee
!
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain ServiceProvider-L4 level 4
 mep archive-hold-time 60
 mip auto-create
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
 mip auto-create
service MetroCustomer1OpA vlan 101
  continuity-check
!
interface
 ethernet cfm mip level 1    <<<< manual MIP
!
interface
 ethernet cfm mip level 4    <<<< manual MIP
 ethernet cfm mep domain OperatorA mpid 102 vlan 101
```

U-PE B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
```

```
!
ethernet cfm domain Customer-L7 level 7
 mip auto-create
 service Customer1 vlan 101 direction down
!
ethernet cfm domain ServiceProvider-L4 level 4
 mep archive-hold-time 60
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorB level 2
 mep archive-hold-time 65
 service MetroCustomer1OpB vlan 101
  continuity-check
!
interface
 ethernet cfm mip level 7   <<<< manual MIP
 ethernet cfm mep domain ServiceProvider-L4 mpid 402 vlan 101
 ethernet cfm mep domain OperatorB mpid 201 vlan 101
!
interface
 ethernet cfm mip level 2   <<<< manual MIP
```

N-PE B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain ServiceProvider level 4
 mep archive-hold-time 60
 mip auto-create
 service MetroCustomer1 vlan 101
  continuity-check
!
ethernet cfm domain OperatorB level 2
 mep archive-hold-time 65
 mip auto-create
 service MetroCustomer1OpB vlan 101
  continuity-check
!
interface
ethernet cfm mip level 2      <<<< manual MIP
!
interface
 ethernet cfm mip level 4     <<<< manual MIP
 ethernet cfm mep domain OperatorB mpid 202 vlan 101
```

CE-B Configuration

```
!
ethernet cfm global
ethernet cfm ieee
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
ethernet cfm domain Customer-L7 level 7
 service Customer1 vlan 101 direction down
  continuity-check
```

```
!
interface
 ethernet cfm mep domain Customer-L7 mpid 702 vlan 101
```

Example: Provisioning CFM over xconnect

This configuration is an example for CFM over xconnect L2 network. The basic topology example:

CE-A --- (gi2.efp2) PE-A (vfi110) --- mpls core --- (vfi110) PE-B (gi4.efp2) --- CE-B

This configuration example shows only CFM-related command on PE-A and PE-B.

PE-A Configuration

```
pseudowire-class vlan-xconnect
 encapsulation mpls
!
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache

ethernet cfm domain ServiceProvider-L2 level 2
service ServiceProvider1 evc EVC1
  continuity-check
!
!
ethernet evc EVC1
!

interface GigabitEthernet2
service instance 2 ethernet EVC1
  encapsulation dot1q 2
  xconnect 1.0.2.1 2 encapsulation mpls pw-class vlan-xconnect
  cfm mep domain ServiceProvider-L2 mpid 4002
 !
!
interface Loopback0
  ip address 1.0.1.1 255.255.255.255
!
```

PE-B Configuration

```
pseudowire-class vlan-xconnect
  encapsulation mpls
!
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache

ethernet cfm domain ServiceProvider-L2 level 2
 service ServiceProvider1 evc EVC1
  continuity-check
 !
!
ethernet evc EVC1
!

interface GigabitEthernet4
 service instance 2 ethernet EVC1
  encapsulation dot1q 2
  xconnect 1.0.1.1 2 encapsulation mpls pw-class vlan-xconnect
```

```
  cfm mep domain ServiceProvider-L2 mpid 6002
 !
!

interface Loopback0
 ip address 1.0.2.1 255.255.255.255
!
```

Example: Provisioning CFM over VPLS

This configuration is an example for CFM over VPLS L2 network. The basic topology example:

CE-A --- (gi2.efp110) PE-A (vfi110) --- mpls core --- (vfi110) PE-B (gi4.efp110) --- CE-B

This configuration example shows only CFM-related command on PE-A and PE-B.

PE-A Configuration

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache

ethernet cfm domain ServiceProvider-L2 level 2
 service ServiceProvider1 evc EVC_IS_N110 vlan 110
  continuity-check
 !
!

ethernet evc EVC_IS_N110
!

bridge-domain 110
 member GigabitEthernet2 service-instance 110
 member vfi vfi110
!

l2vpn vfi context vfi110
 vpn id 110
 l2protocol forward
 evc EVC_IS_N110
 member 50.50.50.50 encapsulation mpls
!

interface GigabitEthernet2
 service instance 110 ethernet EVC_IS_N110
  encapsulation dot1q 110
  cfm mep domain ServiceProvider-L2 mpid 7001
 !
!

interface Loopback30
 ip address 40.40.40.40 255.255.255.255
end
```

PE-B Configuration

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache

ethernet cfm domain ServiceProvider-L2 level 2
 service ServiceProvider1 evc EVC_IS_N110 vlan 110
  continuity-check
 !
```

```
!

ethernet evc EVC_IS_N110
!

bridge-domain 110
 member GigabitEthernet4 service-instance 110
 member vfi vfi110
!

l2vpn vfi context vfi110
 vpn id 110
 l2protocol forward
 evc EVC_IS_N110
 member 40.40.40.40 encapsulation mpls
!

interface GigabitEthernet4
 service instance 110 ethernet EVC_IS_N110
  encapsulation dot1q 110
  cfm mep domain ServiceProvider-L2 mpid 7002
 !
!

interface Loopback30
 ip address 50.50.50.50 255.255.255.255
!
```

Additional References

Related Documents

Related Topic	Document Title
CFM commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network	"Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network"
IP SLAs for Metro Ethernet	"IP SLAs for Metro Ethernet"
ISSU feature and functions	"Cisco IOS Broadband High Availability In Service Software Upgrade"
Performing an ISSU	"Cisco IOS In Service Software Upgrade Process and Enhanced Fast Software Upgrade Process"
SSO	“Stateful Switchover” module of the *High Availability Configuration Guide*

Standards

Standard	Title
IEEE 802.1ag Standard	*802.1ag - Connectivity Fault Management*
IETF VPLS OAM	*L2VPN OAM Requirements and Framework*
ITU-T	*ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks*

MIBs

MIB	MIBs Link
CISCO-ETHER-CFM-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Ethernet CFM for Cisco QFP-based Platforms

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 63: Feature Information for Configuring Ethernet CFM for Cisco QFP-based Platforms

Feature Name	Releases	Feature Information
IEEE 802.1ag-2007 Compliant CFM for QFP-based Platforms	Cisco IOS XE Release 3.2S	IEEE CFM is an end-to-end per-service Ethernet layer OAM protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs. Y.1731 is an ITU-T recommendation for OAM functions in Ethernet-based networks. This feature is the implementation of IEEE 802.1ag Standard-Compliant CFM and Y.1731 in Cisco IOS XE software. The following commands were introduced or modified: **continuity-check**, **ethernet cfm domain level**, **ethernet cfm global**, **ethernet cfm ieee**, **ethernet cfm mep crosscheck**, **ethernet cfm mep crosscheck start-delay**, **ethernet cfm mep domain mpid**, **ethernet cfm traceroute cache**, **ethernet cfm traceroute cache hold-time**, **ethernet cfm traceroute cache size**, **mep archive-hold-time**, **mep mpid**, **service (cfm-srv)**, **snmp-server enable traps ethernet cfm cc**, and **snmp-server enable traps ethernet cfm crosscheck**.
E-OAM : Multiple port MAs under single MD	Cisco IOS XE Release 3.7S	Support for multiple MAs under a single maintenance domain was added. The following commands were introduced or modified: **clear ethernet cfm ais**, **ethernet cfm lck**, **ethernet cfm mep crosscheck**, **ethernet cfm mep domain mpid**, **ping ethernet**, **show ethernet cfm maintenance-points remote**, **show ethernet cfm maintenance-points remote crosscheck**, **show ethernet cfm maintenance-points remote detail**, **show ethernet cfm traceroute-cache**, **traceroute ethernet**.

Glossary

CCM—continuity check message. A multicast CFM frame that a MEP transmits periodically to ensure continuity across the maintenance entities to which the transmitting MEP belongs, at the MA level on which the CCM is sent. No reply is sent in response to receiving a CCM.

EVC—Ethernet virtual connection. An association of two or more user-network interfaces.

fault alarm—An out-of-band signal, typically an SNMP notification, that notifies a system administrator of a connectivity failure.

inward-facing MEP—A MEP that resides in a bridge and transmits to and receives CFM messages from the direction of the bridge relay entity.

maintenance domain—The network or part of the network belonging to a single administration for which faults in connectivity are to be managed. The boundary of a maintenance domain is defined by a set of DSAPs, each of which may become a point of connectivity to a service instance.

maintenance domain name—The unique identifier of a domain that CFM is to protect against accidental concatenation of service instances.

MEP—maintenance endpoint. An actively managed CFM entity associated with a specific DSAP of a service instance, which can generate and receive CFM frames and track any responses. It is an endpoint of a single MA, and terminates a separate maintenance entity for each of the other MEPs in the same MA.

MEP CCDB—A database, maintained by every MEP, that maintains received information about other MEPs in the maintenance domain.

MIP—maintenance intermediate point. A CFM entity, associated with a specific pair of ISS SAPs or EISS Service Access Points, which reacts and responds to CFM frames. It is associated with a single maintenance association and is an intermediate point within one or more maintenance entities.

MIP CCDB—A database of information about the MEPs in the maintenance domain. The MIP CCDB can be maintained by a MIP.

MP—maintenance point. Either a MEP or a MIP.

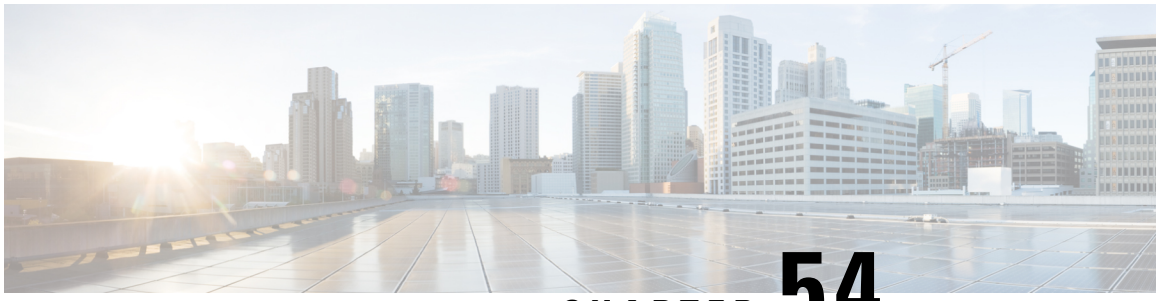
MPID—maintenance endpoint identifier. A small integer, unique over a given MA, that identifies a specific MEP.

OAM—operations, administration, and maintenance. A term used by several standards bodies to describe protocols and procedures for operating, administrating, and maintaining networks. Examples are ATM OAM and IEEE Std. 802.3ah OAM.

operator—Entity that provides a service provider a single network of provider bridges or a single Layer 2 or Layer 3 backbone network. An operator may be identical to or a part of the same organization as the service provider. For purposes of IEEE P802.1ag, Draft Standard for Local and Metropolitan Area Networks, the operator and service provider are presumed to be separate organizations.

Terms such as “customer,” “service provider,” and “operator” reflect common business relationships among organizations and individuals that use equipment implemented in accordance with IEEE P802.1ag.

UNI—user-network interface. A common term for the connection point between an operator's bridge and customer equipment. A UNI often includes a C-VLAN-aware bridge component. The term UNI is used broadly in the IEEE P802.1ag standard when the purpose for various features of CFM are explained. UNI has no normative meaning.



CHAPTER 54

Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Series Router

Ethernet virtual circuit (EVC) infrastructure is a Layer 2 platform-independent bridging architecture that supports Ethernet services. This document describes the infrastructure and the features it supports on the Cisco ASR 1000 Series Aggregation Services Router.

Restrictions for Configuring EVCs on the Cisco ASR 1000 Series Router

- Bridge domain configuration is supported only as part of the EVC service instance configuration.
- The following features are not supported:
  - Service instance (Ethernet flow point [EFP]) group support
  - EVC cross-connect and connect forwarding services
  - Ethernet service protection (Ethernet Operations, Administration, and Maintenance [EOAM], connectivity fault management [CFM], Ethernet Local Management Interface [E-LMI]) on EVCs
  - IPv6 access control lists (ACLs) are not supported.

Information About Configuring EVCs on the Cisco ASR 1000 Series Router

The following topics are described in this section and provide background information for configuring EVCs on the Cisco ASR 1000 Series Router:

In Cisco IOS XE Release 3.2S and later releases, the following features are supported in the EVC infrastructure:

In Cisco IOS XE Release 3.3S, Layer 3 and Layer 4 protocol support was added. This support is described in the "Layer 3 and Layer 4 ACL Support".

EVCs

An EVC is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network. A bridge domain is a local broadcast domain that is VLAN-ID-agnostic. An Ethernet flow point (EFP) service instance is a logical interface that connects a bridge domain to a physical port.

An EVC broadcast domain is determined by a bridge domain and the EFPs that are connected to it. You can connect multiple EFPs to the same bridge domain on the same physical interface, and each EFP can have its own matching criteria and rewrite operation. An incoming frame is matched against EFP matching criteria on the interface, learned on the matching EFP, and forwarded to one or more EFPs in the bridge domain. If there are no matching EFPs, the frame is dropped.

You can use EFPs to configure VLAN translation. For example, if there are two EFPs egressing the same interface, each EFP can have a different VLAN rewrite operation, which is more flexible than the traditional switch port VLAN translation model.

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

Encapsulation (Flexible Service Mapping)

Encapsulation defines the matching criteria that map a VLAN, a range of VLANs, class of service (CoS) bits, Ethertype, or a combination of these to a service instance. VLAN tags and CoS can be a single value, a range, or a list. Ethertype can be a single type or a list of types.

Different types of encapsulations are default, dot1ad, dot1q, priority-tagged, and untagged. On the Cisco ASR 1000 Series Router, priority-tagged frames are always single-tagged. Valid Ethertypes (type) are ipv4, ipv6, pppoe-all, pppoe-discovery, and pppoe-session.

Encapsulation classification options also include:

- inner tag CoS
- inner tag VLAN
- outer tag CoS
- outer tag VLAN
- outer tag Ethertype (VLAN type)--VLAN type is always matched. If you do not specify an alternative, the default is 0x8100 for dot1q and 0x88a8 for dot1ad.
- payload Ethertype--Any Ethertype tag after the VLAN tag

When you configure an encapsulation method, you enable flexible service mapping, which allows you to map an incoming packet to an EFP based on the configured encapsulation.

The default behavior for flexible service mapping based on outer 802.1q and 802.1ad VLAN tag values is nonexact, meaning that when the EFP encapsulation configuration does not explicitly specify an inner (second) VLAN tag matching criterion, the software maps both single-tagged and double-tagged frames to the EFP as long as the frames fulfill the criteria of outer VLAN tag values. The command-line interface (CLI) does allow you to specify exact mapping with the **exact** keyword. If this keyword is specified, the EFP is designated as single-tagged-frame-only and double-tagged frames are not classified to that EFP.

Using the CLI **encapsulation** command in service-instance configuration mode, you can set encapsulation criteria. You must configure one encapsulation command per EFP (service instance). After you have configured an encapsulation method, these commands are available in service instance configuration mode:

- **bridge-domain** --Configures a bridge domain.
- **rewrite** --Configures Ethernet rewrite criteria.

The table below shows the supported encapsulation types.

Table 64: Supported Encapsulation Types

Command	Description
encapsulation dot1q *vlan-id* [**,** *vlan-id* [**-** *vlan-id*]]	Defines the matching criteria to be used to map 802.1q frames ingressing on an interface to the appropriate EFP. The options are a single VLAN, a range of VLANs, or lists of VLANs or VLAN ranges. VLAN IDs are 1 to 4094. • Enter a single VLAN ID for an exact match of the outermost tag. • Enter a VLAN range for a ranged outermost match.
encapsulation dot1q *vlan-id* **second-dot1q** *vlan-id* [**,** *vlan-id* [**-** *vlan-id*]]	Double-tagged 802.1q encapsulation. Matching criteria to be used to map QinQ frames ingressing on an interface to the appropriate EFP. The outer tag is unique and the inner tag can be a single VLAN, a range of VLANs or lists of VLANs or VLAN ranges. • Enter a single VLAN ID in each instance for an exact match of the outermost two tags. • Enter a VLAN range for second-dot1q for an exact outermost tag and a range for a second tag.
encapsulation dot1q {**any** | *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]]} **etype** *ethertype*	Ethertype encapsulation is the payload encapsulation type after VLAN encapsulation. Ethertype encapsulation matches any or an exact outermost VLAN or VLAN range and a payload ethertype. Valid values for *ethertype* are **ipv4**, **ipv6**, **pppoe-discovery**, **pppoe-session**, or **pppoe-all**.
encapsulation dot1q *vlan-id* **cos** *cos-value* **second-dot1q** *vlan-id* **cos** *cos-value*	CoS value encapsulation defines match criteria after including the CoS for the S-Tag and the C-Tag. The CoS value is a single digit between 1 and 7 for S-Tag and C-Tag. You cannot configure CoS encapsulation with the **encapsulation untagged** command, but you can configure it with the **encapsulation priority-tagged** command. The result is an exact outermost VLAN and CoS match and second tag. You can also use VLAN ranges.
encapsulation dot1q any	Matches any packet with one or more VLANs.
encapsulation dot1q vlan-type	Specifies the value of the VLAN protocol type, which is the tag protocol identifier (TPID) of an 802.1q VLAN tag. If there is more than one tag, this command refers to the outermost tag. By default the TPID is assumed to be 0x8100. Use this command to set the TPID to other supported alternatives: 0x88A8, 0x9100, 0x9200.
encapsulation dot1ad	Defines the matching criteria to be used to map 802.1d frames ingressing on an interface to the appropriate EFP.

Command	Description
encapsulation untagged	Matching criteria to be used to map native Ethernet frames (without a dot1q tag) entering an interface to the appropriate EFP. Only one EFP per port can have untagged encapsulation. However, a port that hosts EFP matching untagged traffic can also host other EFPs that match tagged frames.
encapsulation default	Configures the default EFP on an interface, acting as a catch-all encapsulation for all packets without a configured encapsulation. All packets are seen as native. If you enter the **rewrite** command with encapsulation default, the command is rejected. Only one default EFP per interface can be configured. If you try to configure more than one default EFP, the command is rejected.
encapsulation priority-tagged	Specifies priority-tagged frames. A priority-tagged packet has VLAN ID 0 and a CoS value of 0 to 7.

If a packet entering or leaving a port does not match any of the encapsulations on that port, the packet is dropped, resulting in filtering on both ingress and egress. The encapsulation must match the packet on the wire to determine filtering criteria. On the wire refers to packets ingressing the router before any rewrites and to packets egressing the router after all rewrites.

Layer 3 and Layer 4 ACL Support

Beginning in Cisco IOS XE Release 3.3S, support was added for configuring IPv4 Layer 3 and Layer 4 ACLs on EFPs. Configuring an ACL on an EFP is the same as configuring an ACL on other types of interfaces; for example, Ethernet or asynchronous transfer mode (ATM). One exception is that ACLs are not supported for packets prefixed with a Multiprotocol Label Switching (MPLS) header, including when an MPLS packet contains either Layer 3 or Layer 4 headers of supported protocols.

An ACL configured on a main interface containing EFPs does not affect traffic through the EFPs.

To configure an IPv4 Layer 3 and Layer 4 ACL on an EFP, use the **ip access-group** command. An ACL configuration is shown in the "Configuring an ACL on an EFP".

Advanced Frame Manipulation

The Advanced Frame Manipulation feature allows you to specify the VLAN tag manipulation needed on both the incoming and outgoing frames of an EFP. These manipulations include PUSH, POP, and TRANSLATION of one or both VLAN tags.

The PUSH, POP, and TRANSLATION manipulations are as follows:

- PUSH Operations
  - Add one VLAN tag
  - Add two VLAN tags
- POP Operations
  - Remove the outermost VLAN tag
  - Remove the two outermost VLAN tags

- TRANSLATION Operations
  - 1:1 VLAN Translation
  - 1:2 VLAN Translation
  - 2:1 VLAN Translation
  - 2:2 VLAN Translation

When a VLAN tag exists and a new one is added, the CoS field of the new tag is set to the same value as the CoS field of the existing VLAN tag; otherwise, the CoS field is set to a default of 0. Using QoS marking configuration commands, you can change the CoS marking.

EFPs and Layer 2 Protocols

On the Cisco ASR 1000 Series Router, EFPs treat the protocol data units (PDUs) of Layer 2 protocols as data frames. PDUs are forwarded as data frames.

Layer 2 protocols include Cisco Discovery Protocol, Dynamic Trunking Protocol (DTP), Link Aggregation Control Protocol (LACP), Link Layer Discovery Protocol (LLDP), Multiple Spanning Tree Protocol (MSTP), Port Aggregation Protocol (PAgP), Unidirectional Link Detection (UDLD), and VLAN Trunk Protocol (VTP).

Egress Frame Filtering

Egress frame filtering is performed to ensure that frames exiting an EFP contain a Layer 2 header that matches the encapsulation characteristics associated with the EFP. This filtering is done primarily to prevent unintended frame leaks and is always enabled on EFPs.

Bridge Domains

A bridge domain defines a broadcast domain internal to a platform and allows the decoupling of a broadcast domain from a VLAN. This decoupling enables per-port VLAN significance, thus removing the scalability limitations associated with a single per-device VLAN ID space. You can configure a maximum of 4096 EFPs per bridge domain.

A bridge domain interface (BDI) is used to support frame forwarding in a bridge domain at Layer 3. The BDI is a virtual interface that supports Layer 3 features. Each bridge domain can have only one BDI configuration.

If the destination MAC address in a frame received from one of the EFPs participating in a bridge domain matches the BDI MAC address, the frame is routed; otherwise, the frame is bridged. When the egress interface for a routed packet is the BDI interface, the frame is bridged using the destination MAC address.

Frames with broadcast and well-known multicast MAC addresses are also forwarded to the BDI.

The following sections describe support for bridge domains:

EFP, bridge domain, and BDI support based on the Cisco ASR 1000 Series Router forwarding processors are shown in the table in "EFP Bridge Domain and BDI Support Based on the Cisco ASR 1000 Series Router Forwarding Processors".

Ethernet MAC Address Learning

MAC address learning is always enabled and cannot be disabled.

Flooding of Layer 2 Frames for Unknown MAC Multicast and Broadcast Addresses

A Layer 2 frame with an unknown unicast or broadcast destination MAC address is flooded to all the EFPs in the bridge domain except to the originating EFP. A frame with a multicast MAC address is flooded to all the EFPs in the bridge domain. If the destination MAC address is a multicast MAC address, the frame is treated like a broadcast frame and sent to all the EFPs in the bridge domain.

When a frame with either a multicast or broadcast MAC address is flooded and a BDI is associated with the bridge domain, the frame is also flooded to the BDI.

Replication of frames involves recycling the frame several times. This recycling may have a negative effect on forwarding performance and reduce the packet forwarding rate for all features.

Layer 2 Destination MAC Address-Based Forwarding

When bridging is configured, a unicast frame received from an EFP is forwarded based on the destination Layer 2 MAC address. If the destination address is known, the frame is forwarded only to the EFP associated with the destination address.

Because bridge and EFP configurations are interrelated, bridging is supported only on EFPs. To support multiple bridge domains, MAC address entries are associated with the bridge domain of the EFP. Only unicast MAC addresses need to be dynamically learned.

EVC infrastructure does not modify frame contents. Each bridge domain can learn 1000 MAC addresses per second. The Layer 2 frame forwarding rate is 8 million packets per second (MPPS) if flooding is not involved.

MAC Address Aging

The dynamically learned MAC address entries in the MAC table are periodically aged out and entries that are inactive for longer than the configured time period are removed from the table. The supported range of aging-time values, in seconds, is 30 to 600 with a granularity of 1. The default is 5 minutes.

The **aging-time** parameter can be configured per bridge domain and is a relative value. The value is the aging time relative to the time a frame was received with that MAC address.

MAC Address Move

As stations (systems connected to the Cisco ASR 1000 Series Router through the EFP interface) move from one network to another, the interface associated with a MAC address changes.

MAC Address Table

The MAC address table is used to forward frames based on Layer 2 destination MAC addresses. The table consists of static MAC addresses downloaded from the route processor (RP) and the MAC addresses dynamically learned by the data path.

While the MAC Learning feature is enabled, an entry is added to the MAC table when a new unique MAC address is learned on the data path and an entry is deleted from the table when it is aged out.

Split Horizon Group

The split-horizon feature allows service instances in a bridge domain to join groups. Service instances in the same bridge domain and split-horizon group cannot pass data to each other but can forward data to other service instances that are in the same bridge domain and not in the same split-horizon group.

A service instance cannot join more than one split-horizon group. A service instance does not have to be in a split-horizon group. When a service instance does not belong to a group, it can send and receive data from all ports within the bridge domain.

One or more EFPs in a bridge domain may be configured for the same split horizon group, but when a frame is replicated to EFPs, that frame cannot be replicated to EFPs that are within the same split horizon group as the input interface. This restriction applies to MAC address frames that are either known or unknown unicast, broadcast, and multicast frames.

Two split horizon groups per bridge domain are supported on the Cisco ASR 1000 Series Router. You can configure a split horizon group using the **bridge-domain** CLI command with the **split-horizon** and **group** keywords. The group ID can be either 0 or 1.

All members of the bridge-domain that are configured with the same group ID are part of the same split-horizon group. EFPs that are not configured with an explicit group ID do not belong to any group.

EFP Bridge Domain and BDI Support Based on the Cisco ASR 1000 Series Router Forwarding Processors

The table below shows EFP, bridge domain, and BDI support based on the Cisco ASR 1000 Series Router forwarding processors.

Table 65: EFP, Bridge Domain, and BDI Support on the Cisco ASR 1000 Series Router Forwarding Processors

Description	ASR1000-ESP5, ASR 1001, ASR 1002-F (ESP2.5)	ASR1000-ESP10, ASR1000-ESP10-N, ASR1000-ESP20,	ASR1000-ESP40
Maximum EFPs per router	8192	16384	24576
Maximum EFPs per bridge domain	4000	4000	4000
Maximum EFPs per interface	8000	8000	8000
Maximum bridge domains per router	4096	4096	4096
Maximum BDIs per router	4096	4096	4096
Maximum MAC table entries per router	65536	65536	65536
Maximum MAC table entries per bridge domain	16384	16384	16384
Maximum split horizon groups per bridge domain	2	2	2

How to Configure EVCs on the Cisco ASR 1000 Series Router

Configuring an EFP and a Bridge Domain on the Cisco ASR 1000 Series Router

Configuring a service instance on a Layer 2 port creates an EFP on which you can configure EVC features. Perform this task to configure an EFP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation** *encapsulation-type vlan-id*
6. **rewrite ingress tag translate 1-to-1 dot1q** *vlan-id* **symmetric**
7. **bridge-domain** *bridge-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode. • The example shows how to configure Gigabit Ethernet interface 0/1/1 and enter interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode. • The example shows how to configure Ethernet service instance 1.
Step 5	**encapsulation** *encapsulation-type vlan-id* **Example:** `Router(config-if-srv)# encapsulation dot1q 1`	Defines the encapsulation type. • The example shows how to define dot1q as the encapsulation type.
Step 6	**rewrite ingress tag translate 1-to-1 dot1q** *vlan-id* **symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag translate 1-to-1 dot1q 1 symmetric`	(Optional) Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance. • The example shows how to specify translating a single tag defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command with reciprocal adjustment to be done in the egress direction.
Step 7	**bridge-domain** *bridge-id*	Configures the bridge domain.

	Command or Action	Purpose
	Example: `Router(config-if-srv)# bridge-domain 1`	• The example shows how to configure bridge domain 1.
Step 8	**end** **Example:** `Router(config-if-srv)# end`	Returns to privileged EXEC mode.

Configuring an ACL on an EFP

Perform this task to configure an ACL on an EFP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** *access-list-number* | *access-list-name*} {**in** | **out**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode. • The example shows how to configure Gigabit Ethernet interface 0/1/1 and enter interface configuration mode.
Step 4	**ip access-group** *access-list-number* | *access-list-name*} {**in** | **out**} **Example:** `Router(config-if)# ip access-group acl55 in`	Applies an IP access list or object group access control list (OGACL) to an interface or a service policy map. • The example shows how to configure an ACL named acl55 for inbound packets.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for EVCs on the Cisco ASR 1000 Series Router

Example Configuring EFPs on a Gigabit Ethernet Interface

```
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 201
  rewrite ingress tag translate 1-to-1 dot1q 300 symmetric
  bridge-domain 1
 !
 service instance 2 ethernet
  encapsulation default
  bridge-domain 1
 !
 service instance 3 ethernet
  encapsulation priority-tagged
  bridge-domain 2
 !
```

Additional References

Related Documents

Related Topic	Document Title
IEEE CFM	"Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network"
Using OAM	"Using Ethernet Operations, Administration, and Maintenance"
IEEE CFM and Y.1731 commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Standards

Standard	Title
IEEE 802.1ag	*802.1ag - Connectivity Fault Management*
IEEE 802.3ah	*Ethernet in the First Mile*
ITU-T	*ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring EVCs on the Cisco ASR 1000 Series Router

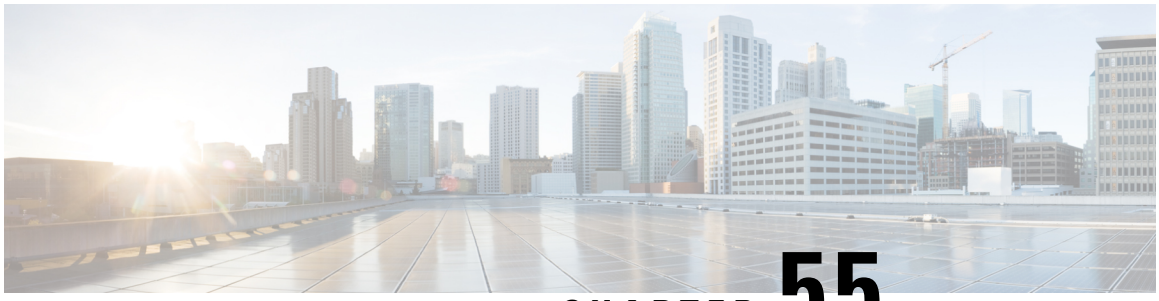
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 66: Feature Information for Configuring EVCs on the Cisco ASR 1000 Series Router

Feature Name	Releases	Feature Information
ASR1000 EVC Infrastructure	Cisco IOS XE Release 3.2S Cisco IOS XE Release 3.3S	EVC infrastructure is a Layer 2 platform-independent bridging architecture that supports Ethernet services. In Cisco IOS XE Release 3.2S, this feature was introduced on the Cisco ASR 1000 Series Router. The following commands are introduced or modified:**rewrite egress tag**, **rewrite ingress tag**, and **shutdown** (bdomain).

Feature Name	Releases	Feature Information
ASR1000 BD Infrastructure	Cisco IOS XE Release 3.2S	Bridge domain infrastructure is a Layer 2 platform-independent architecture that enables bridging. In Cisco IOS XE Release 3.2S this feature was introduced on the Cisco ASR 1000 Series Router. The following sections provide information about support for this feature: The following commands are introduced or modified:**bridge-domain** (service instance), **mac aging-time**.
ACL and QoS Enhancements to EVC Infrastructure in Cisco IOS XE Software	Cisco IOS XE Release 3.3S	Support for configuring Layer 3 and Layer 4 ACLs on EFPs was added in Cisco IOS XE Release 3.3S. The following commands are introduced or modified:**ip access-group**.



CHAPTER 55

Network Interface Device Support

The Network Interface Device (NID) support feature enables support for the NID functionality on a device without including an NID hardware in the network.

Information About NID Support

Network Interface Device Support on the L3 Interface

The Network Interface Device (NID) support feature enables support for the NID functionality on a device without including an NID hardware in the network. This feature combines the Customer-Premises Equipment (CPE) and the NID functionality into a physical device. The following are the advantages of configuring the NID functionality:

- Eliminates the need for a physical NID device and trunk roll.
- Supports both the managed CPE feature set and the NID requirements.

Supported Platforms

The NID Support feature is supported on the following platforms:

- Cisco ISR 4000 Series Integrated Services Routers

Restrictions for NID Support

- Port-channel and EVC interface are not supported .

How to Configure NID Support

Configuring NID Support

Perform the following task to configure NID support:

```
enable
    configure terminal
        interface gigabitEthernet 0/0/2
            no ip address
            port tagging
            encapsulation dot1q 10
            set cos 6
            end
```

Configuration Examples for NID Support

Example: Configuring NID

This configuration example shows how to configure the NID:

```
Device>enable
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if)#port-tagging
Device(config-if-port-tagging)#encapsulation dot1q 10
Device(config-if-port-tagging)#set cos 6
Device(config-if-port-tagging)#end
```

Example: Verifying NID Configuration

Use the following commands to verify the port tagging sessions:

- **show run int**
- **ping**

Use the **show run int** command to display the port tagging sessions:

```
Device#show run interface GigabitEthernet 0/2
Building configuration...
Current configuration : 10585 bytes
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 port-tagging
  encapsulation dot1q 10
  set cos 6
  exit
end
!
```

```
interface GigabitEthernet0/2.1101
encapsulation dot1Q 100
ip address 10.0.2.4 255.255.255.0
!
interface GigabitEthernet0/2.1102
encapsulation dot1Q 100
ip address 10.0.3.4 255.255.255.0
!
```

Use the **ping** command to verify the connectivity with port tagging configured:

```
Device#ping
 10.0.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router#
```

Troubleshooting the NID Configuration

Caution Because debugging output is assigned high priority in the CPU process, it can diminish the performance of the router or even render it unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Note Before you run any of the debug commands listed in the following table, ensure that you run the **logging buffered debugging** command, and then turn off console debug logging using the **no logging console** command.

Table 67: debug Commands for NID Configuration

debug Command	Purpose
debug ethernet nid configuration	Enables debugging of configuration-related issues.
debug ethernet nid packet egress	Enables debugging of packet processing (VLAN tag push) on the egress side.
debug ethernet nid packet ingress	Enables debugging of packet processing (VLAN tag pop) on the ingress side.

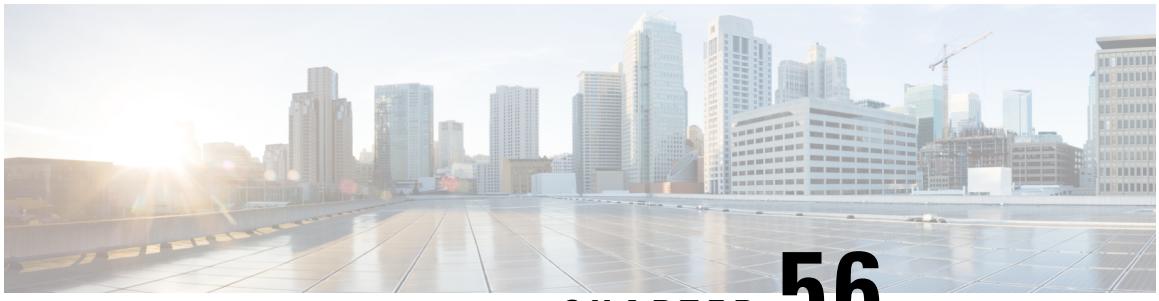
Feature Information for NID Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 68: Feature Information for NID Support

Feature Name	Releases	Feature Information
NID Support	Cisco IOS XE Everest 16.6.1.	The Network Interface Device Support features enables support for the NID functionality on the router without including a NID hardware in the network. No new commands were introduced or modified.



CHAPTER 56

Ethernet Performance Monitoring on Untagged EFPs

The Ethernet Performance Monitoring on untagged EFPs feature enables sessions to run on untagged Ethernet flow points (EFPs).

Information about Ethernet Performance Monitoring on Untagged EFPs

Untagged EFPs

The Ethernet Performance Monitoring on untagged EFPs feature enables sessions to run on untagged Ethernet flow points (EFPs). If an EFP is configured as untagged, then the EFP handles any frames without a dot1q tag, that it receives. Any frames sent using this EFP do not have a dot1q tag.

The dot1q tag contains class of service (CoS) bits, which are used by EPM to test delay or loss of packets with a specific CoS. This support is unavailable when using EPM over untagged EFPs but all other performance monitoring functionality is supported.

How to Configure Ethernet Performance Monitoring on Untagged EFPs

Configuring Ethernet Performance Monitoring on Untagged EFPs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **service instance** *ID* **ethernet***evc-id*
5. **encapsulation untagged**
6. **end**
7. **configure terminal**
8. **ip sla** *operation-number*
9. **ethernet y1731** {**delay** | **loss**} *type* **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | *mac-address target-address*} **cos** *cos-value* {**source** {**mpid** *source-mp-id* | *mac-address tsource-address*}}
10. **exit**
11. **ip sla schedule** *operation-number* **start-time** *time* **life** *life*
12. **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** *type/number* **Example:** `Device(config)# interface GigabitEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 4	**service instance** *ID* **ethernet***evc-id* **Example:** `Device(config-if)# service instance 1 ethernet 50`	Configures a service instance and enters service instance configuration mode.

	Command or Action	Purpose
Step 5	**encapsulation untagged** **Example:** `Device(config-if-srv)# encapsulation untagged`	Sets the encapsulation as untagged.
Step 6	**end** **Example:** `Device(config-if-srv)# end`	Returns to privileged EXEC mode.
Step 7	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 8	**ip sla** *operation-number* **Example:** `Device(config)# ip sla 501`	Configures a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA configuration mode.
Step 9	**ethernet y1731** {**delay** | **loss**} *type* **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | *mac-address target-address*} **cos** *cos-value* {**source** {**mpid** *source-mp-id* | *mac-address tsource-address*}} **Example:** `Device (config-ip-sla)# ethernet y1731 delay DMM domain domain1 evc evc1 mpid 101 cos 0 source mpid 100`	Begins configuring the receiver on the responder and enters IP SLA Y.1731 delay configuration mode. • The source-mp-id or source-address configured by this command corresponds to that of the MEP being configured. **Note** The type argument in the above command syntax takes the following values: DMM, SLM.
Step 10	**exit** **Example:** `Device (config-ip-sla)# exit`	Exits IP SLA configuration mode and returns to privileged EXEC mode.
Step 11	**ip sla schedule** *operation-number* **start-time** *time* **life** *life* **Example:** `Device(config-sla-y1731-delay)# ip sla schedule 501 start-time now life forever`	Begins a probe with a specified operation number starting at the specified timestamp (or 'now' for immediately) for the specified lifetime in seconds (or 'forever' to run until the configuration is removed).
Step 12	**end** **Example:** `Device(config-sla-y1731-delay)# end`	Returns to privileged EXEC mode.

Verifying Ethernet Performance Monitoring on Untagged EFPs

Perform the following task to verify the Ethernet Performance Monitoring on Untagged EFPs

SUMMARY STEPS

1. Enter the **show ip sla statistics** to display performance monitoring sessions with untagged EFPs.

DETAILED STEPS

Enter the **show ip sla statistics** to display performance monitoring sessions with untagged EFPs.

Example:

```
Device# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 5
Loss Statistics for Y1731 Operation 5
Type of operation: Y1731 Loss Measurement
Latest operation start time: *09:08:29.825 PST Wed Jun 11 2014
Latest operation return code: OK
Distribution Statistics:

Interval
 Start time:  *09:08:29.825 PST Wed Jun 11 2014
 Elapsed time: 9 seconds
 Number of measurements initiated: 8
 Number of measurements completed: 8
 Flag: OK
```

Example for Configuring Ethernet Performance Monitoring on Untagged EFPs

Example: Example for Configuring EPM Untagged EFPs

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0
Device(config-if)# service instance 1 ethernet
Device(config-if-srv)# encapsulation untagged
Device(config-if-srv)# end
Device# configure terminal
Device(config)# ip sla 501
Device(config-ip-sla)# ethernet y1731 delay DMM domain domain1 evc evc1 mpid 101 cos 0
source mpid 100
Device(config-sla-y1731-delay)# exit
Device(config)# ip sla schedule 501 start-time now life forever
```

```
Device(config)# end
```

Additional References for Ethernet Performance Monitoring on Untagged EFPs

Related Documents

Related Topic	Document Title
Carrier Ethernet Command Reference	*Cisco IOS Carrier Ethernet Command Reference*
Configuring Ethernet connectivity fault management in a service provider network (Cisco pre-Standard CFM Draft 1)	"Configuring Ethernet Connectivity Fault Management in a Service Provider Network" module in the *Cisco IOS Carrier Ethernet Configuration Guide*
IP SLAs for Metro Ethernet	"IP SLAs for Metro Ethernet"

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

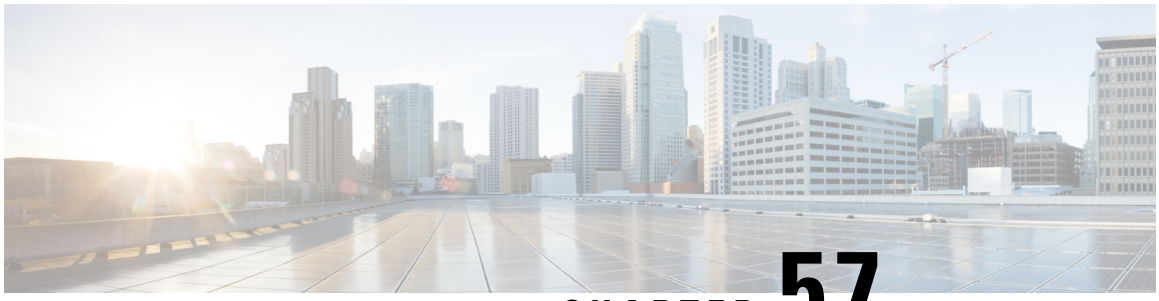
Feature Information for Ethernet Performance Monitoring on Untagged EFPs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 69: Feature Information for Ethernet Performance Monitoring on Untagged EFPs

Feature Name	Releases	Feature Information
Ethernet Performance Monitoring on Untagged EFPs	Cisco IOS Release15.5(2)S	The Ethernet Performance Monitoring on untagged EFPs feature enables sessions to run on untagged Ethernet flow points (EFPs). This feature is enabled on Cisco Aggregation Services ASR 903 Series Routers. No commands were introduced or modified.



CHAPTER 57

Using the IEEE 802.3ad Link Aggregation MIB

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables the bundling of physical interfaces on a physical device to achieve more bandwidth than is available using a single interface. This feature introduces IEEE 802.3ad Link Aggregation (LAG) MIB support in Cisco IOS XE software. The LAG MIB supports the management of interfaces and ports that are part of an LACP port channel and is accessed by a Simple Network Management Protocol (SNMP) manager application.

Prerequisites for Using the IEEE 802.3ad Link Aggregation MIB

- Link aggregation must be configured using the LACP command-line interface (CLI) commands before the MIB tables can be accessed.
- LACP must be supported in the image.

Information About Using the IEEE 802.3ad Link Aggregation MIB

IEEE 802.3ad LAG MIB

The IEEE 802.3ad LAG MIB supports the management of interfaces and ports that are part of an LACP port channel. No specific commands are used to enable the MIB; access is through an SNMP manager application. For information about using SNMP in Cisco IOS XE software, see the “Configuring SNMP Support” chapter of the *Cisco IOS XE Network Management Configuration Guide*, Release 2.

Configuration and Management of LACP bundles

To use the LAG MIB, it is important to know how LACP bundles are configured and managed. For more information about LACP bundles, see the "Configuring IEEE 802.3ad Link Bundling" feature guide.

LAG MIB Table Object Definitions

This section lists the MIB objects and tables that are supported as part of this feature.

dot3adTablesLastChanged Object

The dot3adTablesLastChanged object indicates the time of the most recent change to the dot3adAggTable, dot3adAggPortListTable, or dot3adAggPortTable.

dot3adAggTable

The dot3adAggTable (Aggregator Configuration table) contains information about every aggregator that is associated with a system. Each LACP channel in a device occupies an entry in the dot3adAggTable. Some objects in the table have restrictions, which are described with the object. The objects are described in the table below.

Table 70: Aggregator Configuration Table Objects

Object	Maximum Access/Description
dot3adAggActorAdminKey	Cannot be changed via the SET operation.
dot3adAggActorOperKey	Write access not supported.
dot3adAggActorSystemID	Write access not supported.
dot3adAggActorSystemPriority	Write access not supported.
dot3adAggAggregateOrIndividual	Returns a value of TRUE if more than 1 port is configured in the channel; otherwise, returns a value of FALSE.
dot3adAggCollectorMaxDelay	Cannot be changed via the SET operation.
dot3adAggIndex	Write access not supported.
dot3adAggMACAddress	Write access not supported.
dot3adAggPartnerOperKey	Write access not supported.
dot3adAggPartnerSystemID	Write access not supported.
dot3adAggPartnerSystemPriority	Write access not supported.

dot3adAggPortListTable

The dot3adAggPortListTable (Aggregation Port List table) contains a list of all the ports associated with each aggregator. Each LACP channel in a device occupies an entry in the table. The objects are described in the table below.

Table 71: Aggregation Port List Table Objects

Object	Maximum Access/Description
dot3adAggPortListPorts	Write access not supported.

dot3adAggPortTable

The dot3adAggPortTable (Aggregation Port table) contains LACP configuration information about every aggregation port associated with a device. Each physical port in a device occupies an entry in the dot3adAggPortTable. The objects are described in the table below.

Table 72: Aggregation Port Table Objects

Object	Maximum Access/Description
dot3adAggPortActorAdminKey	Write access not supported.
dot3adAggPortActorAdminState	Write access not supported.
dot3adAggPortActorOperKey	Read-only access supported.
dot3adAggPortActorOperState	Write access not supported.
dot3adAggPortActorPort	Write access not supported.
dot3adAggPortActorPortPriority	Write access not supported.
dot3adAggPortActorSystemID	Write access not supported.
dot3adAggPortActorSystemPriority	Write access not supported.
dot3adAggPortAggregateOrIndividual	Indicates whether a port is attached to an LACP channel. If the port is attached to an LACP channel and the value of the dot3adAggPortAttachedAggID object in the same row is not zero, the value of this object is TRUE. Otherwise, the value is FALSE.
dot3adAggPortAttachedAggID	Write access not supported.
dot3adAggPortIndex	Write access not supported.
dot3adAggPortPartnerAdminKey	Cannot be changed via the SET operation.
dot3adAggPortPartnerAdminPort	Cannot be changed via the SET operation.
dot3adAggPortPartnerAdminPortPriority	Write access not supported.
dot3adAggPortPartnerAdminState	Cannot be changed via the SET operation.
dot3adAggPortPartnerAdminSystemID	Cannot be changed via the SET operation.
dot3adAggPortPartnerAdminSystemPriority	Cannot be changed via the SET operation.
dot3adAggPortPartnerOperKey	Write access not supported.
dot3adAggPortPartnerOperPort	Cannot be changed via the SET operation.
dot3adAggPortPartnerOperPortPriority	Write access not supported.
dot3adAggPortPartnerOperState	Write access is not supported.

Object	Maximum Access/Description
dot3adAggPortPartnerOperSystemID	Write access not supported.
dot3adAggPortPartnerOperSystemPriority	Write access not supported.
dot3adAggPortSelectedAggID	Write access not supported.

dot3adAggPortStatsTable

The dot3adAggPortStatsTable (LACP Statistics table) contains link aggregation information about every port that is associated with a device. Each physical port occupies a row in the table. The objects are described in the table below.

Table 73: LACP Statistics Table Objects

Object	Maximum Access/Description
dot3adAggPortStatsIllegalRx	Write access not supported.
dot3adAggPortStatsLACPDUsRx	Write access not supported.
dot3adAggPortStatsLACPDUsTx	Write access not supported.
dot3adAggPortStatsMarkerPDUsRx	Write access not supported.
dot3adAggPortStatsMarkerPDUsTx	Write access not supported.
dot3adAggPortStatsMarkerResponsePDUsRx	Write access not supported.
dot3adAggPortStatsMarkerResponsePDUsTx	Write access not supported.
dot3adAggPortStatsUnknownRx	Write access not supported.

Additional References

Related Documents

Related Topic	Document Title
Link aggregation configuration tasks	"Configuring IEEE 802.3ad Link Bundling" feature guide
Cisco IOS XE LACP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Configuring SNMP	“Configuring SNMP Support” chapter of the *Cisco IOS XE Network Management Configuration Guide*, Release 2

Related Topic	Document Title
Cisco IOS XE SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*

Standards

Standard	Title
IEEE 802.3ad	*IEEE 802.3ad-2000 Link Aggregation*

MIBs

MIB	MIBs Link
• IEEE 802.3ad MIB • IF MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

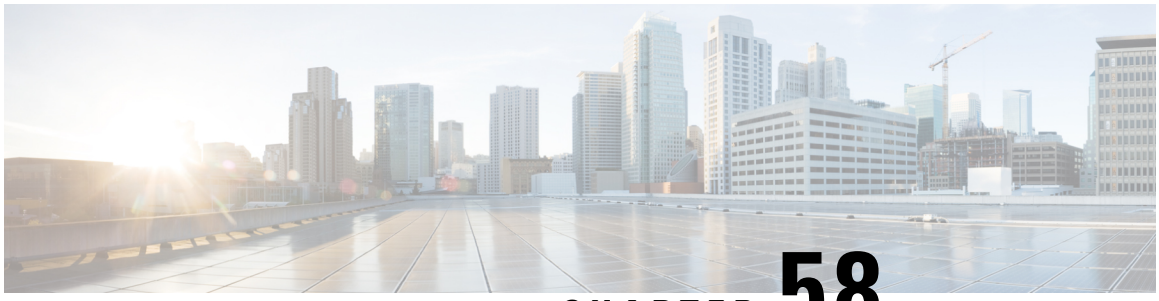
Feature Information for Using the IEEE 802.3ad Link Aggregation MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 74: Feature Information for Using the IEEE 802.3ad Link Aggregation MIB

Feature Name	Releases	Feature Information
IEEE 802.3ad MIB	Cisco IOS XE Release 2.5	This feature introduces LAG MIB support in Cisco IOS XE software. The LAG MIB supports the management of interfaces and ports that are part of an LACP port channel and is accessed by an SNMP manager application. This feature uses no commands.



CHAPTER 58

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

- 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

- 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 maximum of 4 while other platforms support a maximum of 14.
- 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 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.
- 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 75: 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	
	Layer 2 Tunneling Protocol Version 3 (L2TPv3), 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
	PPPoX (PPPoEoE, PPPoEoQinQ, PPPoVLAN)	Supported
3.7.6	Policy-based routing (PBR) over GEC	Supported
3.11	GEC over L2TPv3	Supported

Cisco IOS XE Release	Feature	Bundle Interface
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** *channel-number* **Example:** `Device(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**channel-group** *channel-group-number* **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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Device(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**lacp max-bundle** *max-bundles* **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** *ip-address mask* **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.
Step 7	**show running-config interface port-channel** *group-number* **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: : 110 bytes
!
interface Port-channel10
ip address 172.31.52.10 255.255.255.0
no negotiation auto
lacp max-bundle 3
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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *number* **Example:** `Device(config)# interface port-channel 1`	Specifies the port channel interface and enters interface configuration mode. • *number* —Valid range is from 1 to 64.
Step 4	**ip address** *ip-address mask* **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** *type slot*/*subslot*/ *port* **Example:** `Device(config-if)# interface gigabitethernet`	Specifies the port to bundle.
Step 6	**no ip address** **Example:**	Disables the IP address on the port channel interface.

	Command or Action	Purpose
	`Device(config-if)# no ip address`	
Step 7	**channel-group** *channel-group-number* **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. • *channel-group-number* —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 8	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 9	**interface** *type slot*/*subslot*/ *port* **Example:** `Device(config)# interface gigabitethernet`	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** *channel-group-number* **mode** {**active** | **passive**} **Example:** `Device(config-if)# channel-group 1 mode active`	Assigns the interface to the previously configured port channel group. • *channel-group-number* —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)#
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# exit
Device(config)#
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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**lacp system-priority** *priority* **Example:** `Device(config)# lacp system-priority 200`	Sets the system priority.

	Command or Action	Purpose
Step 4	**interface** *slot/subslot/ port* **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** *priority* **Example:** `Device(config-if)# lacp port-priority 500`	Specifies the priority for the physical interface. • *priority* —Valid range is from 1 to 65535. The higher the number, the lower the priority.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show lacp sys-id** **Example:** `Device# show lacp sys-id`	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 sys-id
200.abdc.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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/subslot/port* **Example:** `Device(config)# interface gigabitethernet`	Configures a Gigabit Ethernet interface.
Step 4	**channel-group** *channel-group-number* **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** *channel-group-number* **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** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no interface port-channel** *number* **Example:** `Device(config)# no interface port-channel 1`	Removes the specified port channel group from a physical port.
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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Creates a port-channel virtual interface and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface port-channel 1`	
Step 4	**lacp min-bundle** *min-bundle* **Example:** `Device(config-if)# lacp min-bundle 1`	Sets the minimum threshold of active links to 1. **Note** For Cisco ASR 1000 Series Aggregation Services Routers, the minimum number of member links per GEC interface is 1 and the maximum number is 14.
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** {*number*	**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-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 : GigabitEthernet , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet , 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
```

The table below describes the significant fields shown in the display.

*Table 76: **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.

Field	Description
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.
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.

Field	Description
packets input	Total number of error-free packets received by the system.
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 terminated 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.
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.

Field	Description
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.
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 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)#
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)#
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)#
Device1(config-if)# channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:07:43.713: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to down
*Aug 20 17:07:44.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet,
changed state to down
*Aug 20 17:07:45.093: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE  Physical Port Link Down
*Aug 20 17:07:45.093: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE  Physical Port Link Down
*Aug 20 17:07:47.093: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to up
*Aug 20 17:07:48.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet,
changed state to up
*Aug 20 17:07:48.957: GigabitEthernet 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 etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - 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: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)
```

```
RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended

Device1# show running-config int po1
Building configuration...

Current configuration : 87 bytes
!
interface Port-channel1
 no ip address
 lacp fast-switchover
 lacp max-bundle 1
end

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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
   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 : GigabitEthernet , 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 runts, 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
                            LACP port     Admin     Oper    Port        Port
```

```
Port      Flags   State     Priority      Key       Key     Number      State
   SA      bndl      32768         0x5       0x5     0x43        0x3D
Device1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device1(config)#
Device1(config-if)# channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:10:19.057: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to down
*Aug 20 17:10:19.469: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE  Physical Port Link Down
*Aug 20 17:10:19.473: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE  Physical Port Link Down
*Aug 20 17:10:21.473: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to up
*Aug 20 17:10:21.473: GigabitEthernet taken out of port-channel5
*Aug 20 17:10:23.413: GigabitEthernet 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: GigabitEthernet 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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
   SA      bndl      32768         0x5       0x5     0x43        0x3D
   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 : GigabitEthernet , Full-duplex, 1000Mb/s  <---- added to port channel
bundle
        Member 1 : GigabitEthernet , 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 runts, 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)#
```

```
Device1(config-if)# no channel-group 5 mode active
Device1(config-if)#
*Aug 20 17:15:49.433: GigabitEthernet taken out of port-channel5
*Aug 20 17:15:49.557: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE  Physical Port Link Down
*Aug 20 17:15:50.161: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE  Physical Port Link Down
*Aug 20 17:15:51.433: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to down
*Aug 20 17:15:52.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet,
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  Physical Port Link Down
*Aug 20 17:15:59.257: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE  Physical Port Link Down
Device1#
*Aug 20 17:16:01.257: %LINK-3-UPDOWN: Interface GigabitEthernet, changed state to up
*Aug 20 17:16:02.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet,
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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
   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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
   SA      bndl      32768         0x5       0x5     0x42        0x3D
Device1# show lacp 5 counters
            LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 5
     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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
   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:
          Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State     Port Priority Admin Key Oper Key Port Number Port State
   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
     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 : GigabitEthernet , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet , 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
```

Additional References Configuring IEEE 802.3ad Link Bundling

Related Documents

Related Topic	Document Title
Configuring EtherChannels	"Configuring Layer 3 and Layer 2 EtherChannel" chapter of the *Catalyst 6500 Release 12.2SXF Software Configuration Guide*
LACP commands	Cisco IOS Carrier Ethernet Command Reference
LACP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Network Management Command Reference

Standards

Standard	Title
IEEE 802.3ad-2000	*IEEE 802.3ad-2000 Link Aggregation*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring IEEE 802.3ad Link Bundling

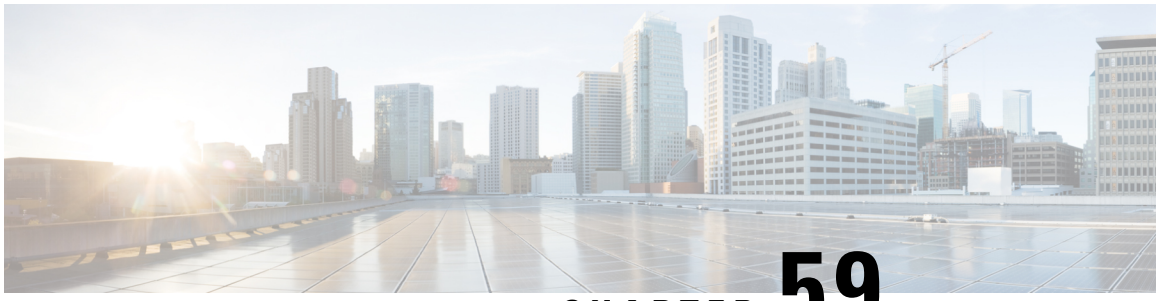
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 77: Feature Information for Configuring IEEE 802.3ad Link Bundling

Feature Name	Releases	Feature Information
EtherChannel Min-Links	Cisco IOS XE Release 2.5 Cisco IOS XE Release 3.8S	The EtherChannel Min-Links feature allows a port channel to be shut down when the number of active links falls below the minimum threshold. Using the **lacp min-bundle** command, you can configure the minimum threshold. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router. The following commands were introduced or modified: **lacp min-bundle**.
IEEE 802.3ad Faster Link Switchover Time	Cisco IOS XE Release 2.5	The IEEE 802.3ad Faster Link Switchover Time feature provides a link failover time of 250 milliseconds or less and a maximum link failover time of 2 seconds. Also, port channels remain in the LINK_UP state to eliminate reconvergence by the Spanning-Tree Protocol. The following commands were introduced or modified: **lacp fast-switchover**.

Feature Name	Releases	Feature Information
IEEE 802.3ad Link Aggregation (LACP)	Cisco IOS XE Release 2.4	The IEEE 802.3ad Link Aggregation feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. In addition, this feature 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. In Cisco IOS XE Release 2.4, this feature was implemented on the Cisco ASR1000 Series Router. The following commands were introduced or modified: **channel-group (interface)**, **debug lacp**, **lacp max-bundle**, **lacp port-priority**, **lacp system-priority**, **show lacp**.
Link Aggregation Control Protocol (LACP) (802.3ad) for Gigabit Interfaces	Cisco IOS XE Release 2.5	The LACP (802.3ad) for Gigabit Interfaces feature bundles individual Gigabit Ethernet links into a single logical link that provides the aggregate bandwidth of up to four physical links. The following commands were introduced or modified: **lacp max-bundle**.
SSO - LACP	Cisco IOS XE Release 2.5	The SSO - LACP feature supports stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles. This feature uses no new or modified commands.
Support for 14 Member-links per GEC Bundle	Cisco IOS XE Denali 16.3.1	The Support for 14 Member-links per GEC Bundle feature extends the number of supported member links from 4 to 14 on Cisco ASR 1000 Series Aggregation Services Routers. This feature uses no new or modified commands.



CHAPTER 59

ITU-T Y.1731 Performance Monitoring in a Service Provider Network

ITU-T Y.1731 performance monitoring provides standard-based Ethernet performance monitoring that encompasses the measurement of Ethernet frame delay, frame-delay variation, and throughput as outlined in the ITU-T Y.1731 specification and interpreted by the Metro Ethernet Forum (MEF). Service providers offer service level agreements (SLAs) that describe the level of performance customers can expect for services. This document describes the Ethernet performance management aspect of SLAs.

Prerequisites for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

- IEEE-compliant connectivity fault management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.

Note Y1731 is supported over Port Channel interfaces.

Information About ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Frame Delay and Frame-Delay Variation

The Frame Delay parameter can be used for on-demand OAM measurements of frame delay and frame-delay variation. When a maintenance end point (MEP) is enabled to generate frames with frame-delay measurement (ETH-DM) information, it periodically sends frames with ETH-DM information to its peer MEP in the same maintenance entity. Peer MEPs perform frame-delay and frame-delay variation measurements through this periodic exchange during the diagnostic interval.

An MEP requires the following specific configuration information to support ETH-DM:

- MEG level—MEG level at which the MEP exists
- Priority
- Drop eligibility—marked drop ineligible
- Transmission rate
- Total interval of ETH-DM
- MEF10 frame-delay variation algorithm

A MEP transmits frames with ETH-DM information using the TxTimeStampf information element. TxTimeStampf is the time stamp for when the ETH-DM frame was sent. A receiving MEP can compare the TxTimeStampf value with the RxTimef value, which is the time the ETH-DM frame was received, and calculate one-way delay using the formula *frame delay = RxTimef – TxTimeStampf*.

One-way frame-delay measurement (1DM) requires that clocks at both the transmitting MEP and the receiving MEPs are synchronized. Measuring frame-delay variation does not require clock synchronization and the variation can be measured using 1DM or a frame-delay measurement message (DMM) and a frame-delay measurement reply (DMR) frame combination.

If it is not practical to have clocks synchronized, only two-way frame-delay measurements can be made. In this case, the MEP transmits a frame containing ETH-DM request information and the TxTimeStampf element, and the receiving MEP responds with a frame containing ETH-DM reply information and the TxTimeStampf value copied from the ETH-DM request information.

Two-way frame delay is calculated as *(RxTimeb–TxTimeStampf)–(TxTimeStampb–RxTimeStampf)*, where RxTimeb is the time that the frame with ETH-DM reply information was received. Two-way frame delay and variation can be measured using only DMM and DMR frames.

To allow more precise two-way frame-delay measurement, the MEP replying to a frame with ETH-DM request information can also include two additional time stamps in the ETH-DM reply information:

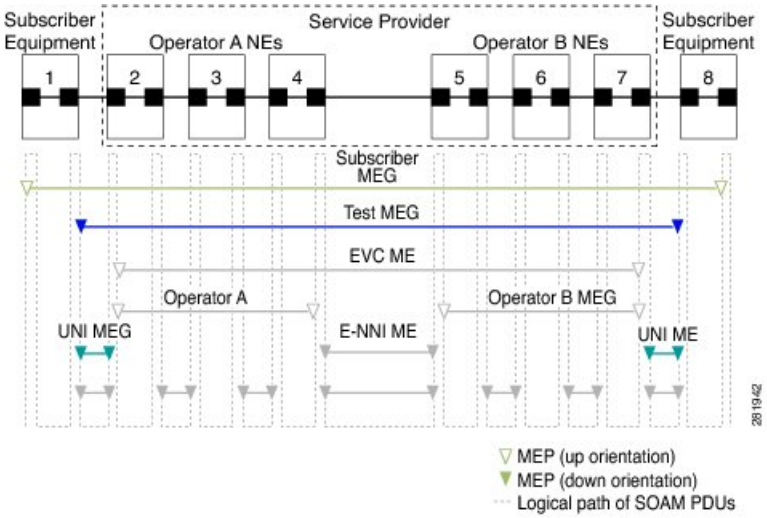
- RxTimeStampf—Time stamp of the time at which the frame with ETH-DM request information was received.
- TxTimeStampb—Time stamp of the time at which the transmitting frame with ETH-DM reply information was sent.
- The timestamping happens at the hardware level for DMM operations.

Note The frame-loss, frame-delay, and frame-delay variation measurement processes are terminated when faults related to continuity and availability occur or when known network topology changes occur.

An MIP is transparent to the frames with ETH-DM information; therefore, an MIP does not require information to support the ETH-DM function.

The figure below shows a functional overview of a typical network in which Y.1731 performance monitoring is used.

Figure 37: Y.1731 Performance Monitoring



Benefits of ITU-T Y.1731 Performance Monitoring

Combined with IEEE-compliant connectivity fault management (CFM), Y.1731 performance monitoring provides a comprehensive fault management and performance monitoring solution for service providers. This comprehensive solution in turn lessens service providers' operating expenses, improves their service-level agreements (SLAs), and simplifies their operations.

How to Configure ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Configuring Performance Monitoring Parameters

The following new commands were introduced that can be used to configure and display performance monitoring parameters: **debug ethernet cfm pm**, **monitor loss counters**, and **show ethernet cfm pm**.

For more information about CFM and Y.1731 performance monitoring commands, see the *Cisco IOS Carrier Ethernet Command Reference*. For more information about debug commands, see the *Cisco IOS Debug Command Reference*.

Configuration Examples for Configuring ITU-T Y.1731 Performance Monitoring Functions

Example: Configuring Performance Monitoring

For Y.1731 performance monitoring configuration examples, see Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations. For information on Y.1731 On-Demand and Concurrent Operations see, IPSLA Y1731 On-Demand and Concurrent Operations.

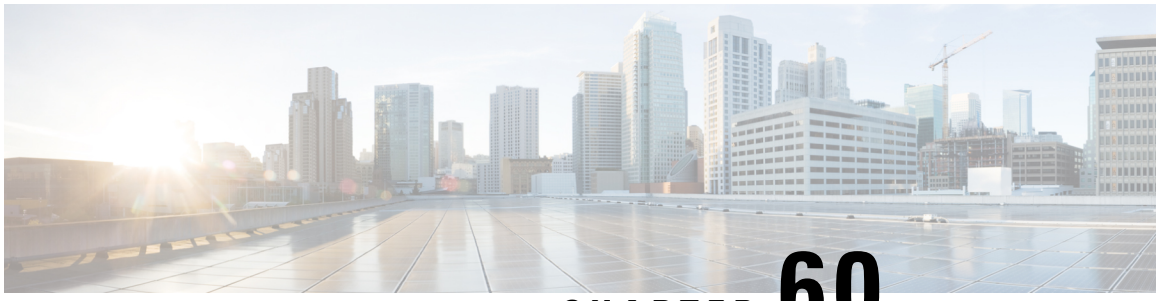
Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 78: Feature Information for ITU-T Y.1731 Performance Monitoring in a Service Provider Network

Feature Name	Releases	Feature Information
Y.1731 Performance Monitoring	Cisco IOS XE Release 3.5S	The Y.1731 Performance Monitoring feature describes the Ethernet performance monitoring aspect of SLAs such as frame loss, frame delay, and frame-delay variation. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. In Cisco IOS XE Release 3.6S, support for port channels and cross connect functionality was provided. The following commands were introduced or modified: **debug ethernet cfm pm**, **ethernet cfm distribution enable**, **monitor loss counters**, **show ethernet cfm pm**.



CHAPTER 60

Enabling Ethernet Local Management Interface

Ethernet Local Management Interface (LMI) is an Ethernet layer operation, administration, and management (OAM) protocol. It provides information that enables autoconfiguration of customer edge (CE) devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC and a user-network interface (UNI) to a CE device.

The advent of Ethernet as a MAN and WAN technology imposes a new set of OAM requirements on Ethernet's traditional operations, which were centered on enterprise networks only. The expansion of Ethernet technology into the domain of service providers, where networks are substantially larger and more complex than enterprise networks and the user-base is wider, makes operational management of link uptime crucial. More importantly, the timeliness in isolating and responding to a failure becomes mandatory for normal day-to-day operations, and OAM translates directly to the competitiveness of the service provider.

Prerequisites for Enabling Ethernet Local Management Interface

Business Requirements

- Ethernet operation, administration, and management (OAM) such as connectivity fault management (CFM) must be implemented and operational on the service provider’s network.

Restrictions for Enabling Ethernet Local Management Interface

- Ethernet Local Management Interface (LMI) relies on Ethernet connectivity fault management (CFM) for the status of an Ethernet virtual circuit (EVC), the remote user network interface (UNI) identifier associated with an EVC, and remote UNI status.
- Ethernet LMI customer edge (CE) is available only on routing ports on routing platforms. For information about Ethernet LMI provider edge (PE) functionality on switching platforms, see the "Configuring Ethernet CFM and E-LMI" chapter of the *Cisco ME 3400 Switch Software Configuration Guide*.
- Not all Cisco software releases support autoconfiguration of CE devices.

Information About Enabling Ethernet Local Management Interface

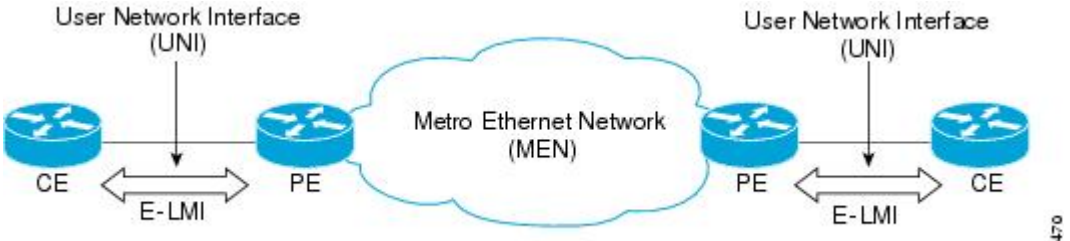
EVC

An Ethernet virtual circuit (EVC) as defined by the Metro Ethernet Forum could be a port level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by the customer edge (CE) device to find an alternative path in to the service provider network or in some cases, fall back to a backup path over Ethernet or another alternative service such as ATM.

Ethernet LMI

Ethernet Local Management Interface (LMI) is an Ethernet layer operation, administration, and management (OAM) protocol between a customer edge (CE) device and the provider edge (PE) device in large Ethernet MANs and WANs. It provides information that enables service providers to autoconfigure CE devices with service parameters and parameter changes from a user provider edge (UPE) device.

The figure below shows where in a network Ethernet LMI functions.



LMI also provides the status of Ethernet virtual circuits (EVCs) in large Ethernet MANs and WANs to the CE. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates EVC and user network identifier (UNI) attributes to a CE device.

The Ethernet LMI protocol includes the following procedures, as defined by the MEF 16 Technical Specification:

- Notifying the CE when an EVC is added
- Notifying the CE when an EVC is deleted
- Notifying the CE of the availability state of a configured EVC (Active, Not Active, or Partially Active)
- Communicating UNI and EVC attributes to the CE

Benefits of Ethernet LMI

- Communication of end-to-end status of the EVC to the CE device
- Communication of EVC and UNI attributes to a CE device
- Competitive advantage for service providers

How to Enable Ethernet Local Management Interface

Enabling Ethernet LMI on All Supported Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet lmi global**
4. **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	**ethernet lmi global** **Example:** `Device(config)# ethernet lmi global`	Enables Ethernet Local Management Interface (LMI) on all supported interfaces on the device.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device# end`	

Enabling Ethernet LMI on a Single Supported Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet lmi interface**
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** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ethernet lmi interface** **Example:** `Device(config-if)# ethernet lmi interface`	Enables Ethernet Local Management Interface (LMI) on the interface.
Step 5	**end** **Example:** `Device# end`	Returns to privileged EXEC mode.

Configuration Examples for Ethernet Local Management Interface

The examples in this section show the configurations that enable Ethernet LMI on all interfaces on a CE device (globally) and on a specific interface on a CE device.

Example: Enabling Ethernet LMI on All Supported Interfaces

```
enable
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ethernet lmi global
end
00:06:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed p
```

Example: Enabling Ethernet LMI on a Single Supported Interface

```
enable
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
interface ethernet 0/0
ethernet lmi interface
end
00:05:51: %SYS-5-CONFIG_I: Configured from console by console
```

Additional References for Enabling Ethernet Local Management Interface

Related Documents

Related Topic	Document Title
Ethernet Connectivity Fault Management (CFM)	"Configuring Ethernet Connectivity Fault Management in a Service Provider Network" in the *Cisco IOS Carrier Ethernet Configuration Guide*
Configuring CFM and Ethernet Local Management Interface (E-LMI) in a service provider network	*Cisco ME 3400 Switch Software Configuration Guide, Rel. 12.2(25)SEG*
Commands used for configuring Ethernet LMI in a service provider network	*Cisco ME 3400 Switch Command Reference, Rel. 12.2(25)SEG*
Ethernet LMI at a provider edge	"Configuring Ethernet Local Management Interface at a Provider Edge" in the *Carrier Ethernet Configuration Guide*

Related Topic	Document Title
Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Standards

Standard	Title
Metro Ethernet Forum 16 Technical Specification	Technical Specification MEF 16- Ethernet Local Management Interface
IEEE P802.1ag/D5.2	*Draft Standard for Local and Metropolitan Area Networks*
ITU-T Q.3/13	Liaison statement on Ethernet OAM (Y.17ethoam)
IETF VPLS OAM	*L2VPN OAM Requirements and Framework*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Enabling Ethernet Local Management Interface

Table 79: Feature Information for Enabling Ethernet Local Management Interface

Feature Name	Releases	Feature Information
Ethernet Local Management Interface	Cisco IOS XE Release 3.9S	Ethernet LMI is an Ethernet layer OAM protocol. It provides information that enables autoconfiguration of CE devices and provides the status of EVCs for large Ethernet MANs and WANs. The following commands were introduced or modified: **clear ethernet lmi statistics**, **debug ethernet lmi**, **ethernet lmi**, **ethernet lmi global**, **ethernet lmi interface**, **show ethernet lmi**.

Glossary

CE --customer edge. Edge equipment on the customer side of a user-network interface (UNI).

CE-VLAN ID --Identifier of a CE-VLAN.

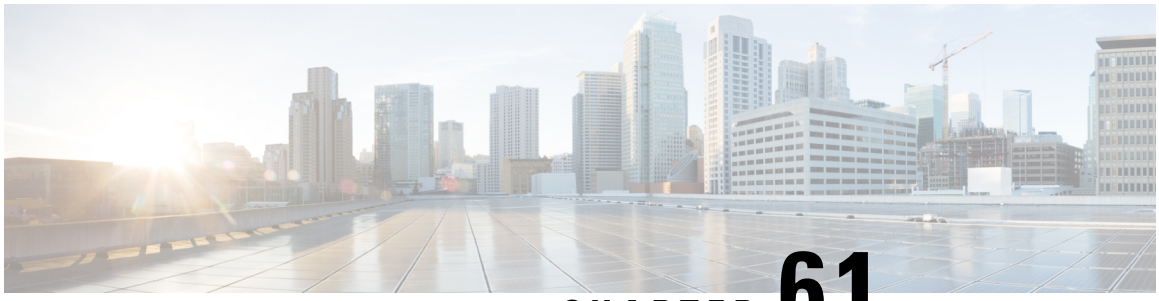
E-LMI --Ethernet Local Management Interface. An Ethernet layer OAM protocol. It provides information that enables autoconfiguration of CE devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet MANs and WANs.

EVC --Ethernet virtual connection. An association of two or more user-network interfaces.

OAM --operations, administration, and maintenance. A term used by several standards bodies to describe protocols and procedures for operating, administrating, and maintaining networks. Examples are ATM OAM and IEEE Std. 802.3ah OAM.

PE --provider edge. Edge equipment on the service provider side of a user-network interface (UNI).

UNI --user-network interface. A common term for the connection point between an operator's bridge and customer equipment. A UNI often includes a C-VLAN-aware bridge component. The term UNI is used broadly in the IEEE P802.1ag/D5.2 standard when the purpose for various features of LMI are explained.



CHAPTER 61

Layer 2 Access Control Lists on EVCs

The ability to filter packets in a modular and scalable way is important for both network security and network management. Access Control Lists (ACLs) provide the capability to filter packets at a fine granularity. In Metro Ethernet networks, ACLs are directly applied on Ethernet virtual circuits (EVCs).

Layer 2 Access Control Lists on EVCs is a security feature that allows packet filtering based on MAC addresses. This module describes how to implement ACLs on EVCs.

Prerequisites for Layer 2 Access Control Lists on EVCs

- Knowledge of how service instances must be configured.
- Knowledge of extended MAC ACLs and how they must be configured.

Restrictions for Layer 2 Access Control Lists on EVCs

Information About Layer 2 Access Control Lists on EVCs

EVCs

An Ethernet virtual circuit (EVC) as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. It is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. An EVC contains the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a specified port.

Service instances are configured under a port channel. The traffic carried by the service instance is load balanced across member links. Service instances under a port channel are grouped and each group is associated with one member link. Ingress traffic for a single EVC can arrive on any member of the bundle. All egress traffic for a service instance uses only one of the member links. Load balancing is achieved by grouping service instances and assigning them to a member link.

Ethernet virtual connection services (EVCS) uses the EVCs and service instances to provide Layer 2 switched Ethernet services. EVC status can be used by a customer edge (CE) device either to find an alternative path to the service provider network or in some cases, to fall back to a backup path over Ethernet or over another alternative service such as ATM.

For information about the Metro Ethernet Forum standards, see the Standards table in the "Additional References" section.

Relationship Between ACLs and Ethernet Infrastructure

The following points capture the relationship between ACLs and Ethernet Infrastructure (EI):

- ACLs can be directly applied on an EVC using the command-line interface (CLI). An ACL is applied to a service instance, which is the instantiation of an EVC on a given port.
- One ACL can be applied to more than one service instance at any time.
- One service instance can have one ACL at most applied to it at any time. If a Layer 2 ACL is applied to a service instance that already has a Layer 2 ACL, the new one replaces the old one.
- Only named ACLs can be applied to service instances. The command syntax ACLs is retained; the **mac access-list extended** command is used to create an ACL.
- The command can be used to provide details about ACLs on service instances.

How to Configure Layer 2 Access Control Lists on EVCs

Creating a Layer 2 ACL

Perform this task to create a Layer 2 ACL with a single ACE.

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 **mac access-list extended** *name*

Example:

```
Device(config)# mac access-list extended test-12-acl
```

Defines an extended MAC ACL and enters mac access list control configuration mode.

Step 4 **permit** {{*src-mac mask* | **any**} {*dest-mac mask* | **any**} [*protocol* [**vlan** *vlan*] [*cos value*]]}

Example:

```
Device(config-ext-macl)# permit 00aa.00bb.00cc 0.0.0 any
```

Allows forwarding of Layer 2 traffic if the conditions are matched. Creates an ACE for the ACL.

Applying a Layer 2 ACL to a Service Instance

Perform this task to apply a Layer 2 ACL to a service instance. Note that packet filtering takes place only after the ACL has been created and applied to the service instance.

Before you begin

Before applying an ACL to a service instance, you must create it using the **mac access-list extended command. See the "Creating a Layer 2 ACL" section.**

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** *type number*

Example:

```
Device(config)# interface gigabitethernet 1/0/0
```

Specifies the type and location of the interface to configure, where:

- *type* --Specifies the type of the interface.
- *number* --Specifies the location of the interface.

Step 4 **service instance** *id* ethernet

Example:

```
Device(config-if)# service instance 100 ethernet
```

Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.

Step 6 **mac access-group** *access-list-name* in

Example:

```
Device(config-if-srv)# mac access-group test-12-acl in
```

Applies a MAC ACL to control incoming traffic on the interface.

Configuring a Layer 2 ACL with ACEs on a Service Instance

Perform this task to configure the same ACL with three ACEs and stop all other traffic on a service instance.

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 **mac access-list extended** *name*

Example:

```
Device(config)# mac access list extended test-12-acl
```

Defines an extended MAC ACL and enters mac access control list configuration mode.

Step 4 **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}

Example:

```
Device(config-ext-macl)# permit 00aa.bbcc.ddea 0.0.0 any
```

Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.

Step 5 **permit** {*src-mac mask* | **any**} {*dest-mac mask* | **any**}

Example:

```
Device(config-ext-macl)# permit 00aa.bbcc.ddeb 0.0.0 any
```

Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.

Step 6 **permit** {*src-mac mask* | **any**} {*dest-mac mask*} | **any**}

Example:

```
Device(config-ext-macl)# permit 00aa.bbcc.ddec 0.0.0 any
```

Allows forwarding of Layer 2 traffic if the conditions are matched. This creates an ACE for the ACL.

Step 7 **deny any any**

Example:

```
Device(config-ext-macl)# deny any any
```

Prevents forwarding of Layer 2 traffic except for the allowed ACEs.

Step 8 **exit**

Example:

```
Device(config-ext-macl)# exit
```

Exits the current command mode and returns to global configuration mode.

Step 9 **interface** *type number*

Example:

```
Device(config)# interface gigabitethernet 1/0/0
```

Specifies the interface.

Step 10 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 200 ethernet
```

Configures an Ethernet service instance on an interface and enters service instance configuration mode.

Step 11 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.

Step 12 **mac access-group** *access-list-name* **in**

Example:

```
Device(config-if-srv)# mac access-group test-12-acl in
```

Applies a MAC ACL to control incoming traffic on the interface.

Verifying the Presence of a Layer 2 ACL on a Service Instance

Perform this task to verify that a Layer 2 ACL is present on an EVC. This verification task can be used after an ACL has been configured to confirm its presence.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance id** *id* **interface** *type* *number* detail

Example:

```
Device# show ethernet service instance id 100 interface gigabitethernet 3/0/1 detail
```

Displays detailed information about Ethernet customer service instances.

Configuration Examples for Layer 2 Access Control Lists on EVCs

Example Applying a Layer 2 ACL to a Service Instance

The following example shows how to apply a Layer 2 ACL called mac-20-acl to a service instance. The ACL has five permitted ACEs and all other traffic is not allowed.

```
enable
configure terminal
 mac access-list extended mac-20-acl

 permit 00aa.bbcc.adec 0.0.0 any

 permit 00aa.bbcc.bdec 0.0.0 any

 permit 00aa.bbcc.cdec 0.0.0 any

 permit 00aa.bbcc.edec 0.0.0 any

 permit 00aa.bbcc.fdec 0.0.0 any

 deny any any
 exit
interface gigabitethernet 10/0/0
 service instance 100 ethernet
 encapsulation dot1q 100
 mac access-group mac-20-acl in
```

Example Applying a Layer 2 ACL to Three Service Instances on the Same Interface

The following example shows how to apply a Layer 2 ACL called mac-07-acl to three service instances on the same interface:

```
enable
configure terminal
mac access-list extended mac-07-acl

permit 00aa.bbcc.adec 0.0.0 any

permit 00aa.bbcc.bdec 0.0.0 any

permit 00aa.bbcc.cdec 0.0.0 any

deny any any
exit
interface gigabitethernet 10/0/0
service instance 100 ethernet
encapsulation dot1q 100
mac access-group mac-07-acl in
service instance 101 ethernet
encapsulation dot1q 101
mac access-group mac-07-acl in
service instance 102 ethernet
encapsulation dot1q 102
mac access-group mac-07-acl in
```

Example Creating a Layer 2 ACL with ACEs

The following example shows how to create a Layer 2 ACL called mac-11-acl with two permitted ACEs:

```
enable
configure terminal
mac access-list extended mac-11-acl
permit 00aa.00bb.00cc 1a11.0101.11c1 any
permit 00aa.00bb.00cc 1a11.0101.11c2 any
```

Example Displaying the Details of a Layer 2 ACL on a Service Instance

The following sample output displays the details of a Layer 2 ACL called test-acl on a service instance.

The table below describes the significant fields in the output.

Table 80: show ethernet service instance Field Descriptions

Field	Description
Service Instance ID	Displays the service instance ID.
L2 ACL (inbound):	Displays the ACL name.
Associated Interface:	Displays the interface details of the service instance.
Associated EVC:	Displays the EVC with which the service instance is associated.
CEVlans:	Displays details of the associated VLAN ID.
State:	Displays whether the service instance is in an up or down state.
L2 ACL permit count:	Displays the number of packet frames allowed to pass on the service instance by the ACL.
L2 ACL deny count	Displays the number of packet frames not permitted to pass on the service instance by the ACL.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Configuring CFM over an EFP Interface with the Cross Connect feature on the Cisco ASR 903 Router.	*Configuring the CFM over EFP Interface with Cross Connect Feature*

Related Topic	Document Title
Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router	*Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router*

Standards

Standard	Title
MEF 6.1	*Metro Ethernet Services Definitions Phase 2 (PDF 6/08)*
MEF 10.1	*Ethernet Services Attributes Phase 2 (PDF 10/06)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

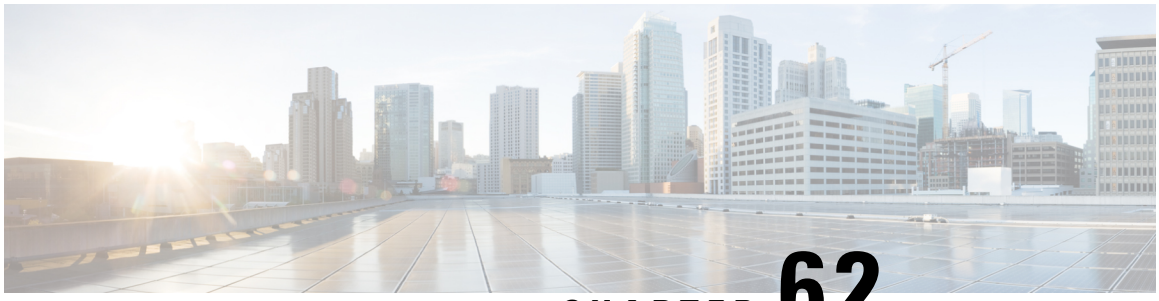
Feature Information for Layer 2 Access Control Lists on EVCs

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 81: Feature Information for Layer 2 Access Control Lists on EVCs

Feature Name	Releases	Feature Information
Layer 2 Access Control Lists on EVCs	Cisco IOS XE Release 3.6S	The Layer 2 Access Control Lists on EVCs feature introduces ACLs on EVCs. • The following commands were introduced or modified: **interface, mac access-group in**, **mac access-list extended, show ethernet service instance**.



CHAPTER 62

Layer 2 Ethernet over GRE

Ethernet over Soft Generic Routing Encapsulation (EoGRE) is an aggregation solution for aggregating WiFi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic from an end host, and encapsulates the traffic in Ethernet packets over an IP GRE tunnel. The IP GRE tunnel terminates on a service provider broadband network gateway, which then terminates the end host traffic and manages the subscriber session for the end host.

Restrictions for Layer 2 Ethernet over GRE

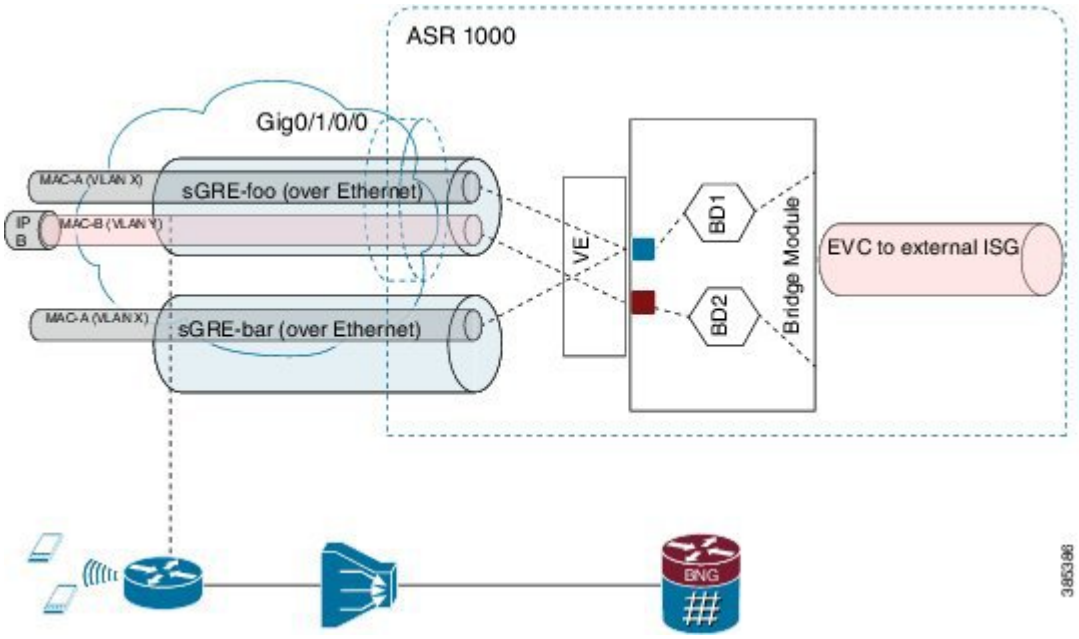
- Transport on IPv6 is not supported.
- Virtual Ethernet interface does not support encapsulation untagged.
- L2 EoGRE is only supported on Cisco ASR 1000 routers. It is not supported on Cisco CSR1000V or Cisco 4000 Series ISR routers.
- Multicast traffic is not supported.

Information About Layer 2 Ethernet over GRE

The ASR 1000 platform services as the SP broadband network gateway which:

- Terminates the IP GRE tunnel, and/or
- Manages the subscriber session for the end-host client.

Figure 38: Ethernet over Soft GRE Deployment



The deployment model that is supported is the two-box model:

- In the two-box model, the ASR 1000 router provides only the functionality to terminate the bridged Ethernet over soft GRE traffic. The ISG subscriber management resides in an external router which is connected with the router using L2 bridge-domain.

The major components involved in L2 EoGRE are:

- Virtual Ethernet interface.
- Ethernet service instance.
- IP GRE tunnel data plane.
- L2 bridge-domain data plane.

Control Plane—After the Virtual Ethernet interface is configured, the Virtual Ethernet interface is downloaded to the ASR 1000 platform as a virtual interface.

Service instances (EVCs) are configured under the virtual ethernet interface and are downloaded to ASR1K platform. The service instances are then propagated in the ASR 1000 platform to fman-rp, fman-fp, cpp-client and cpp dataplane, where the EVC feature invocation arrays (FIAs) are enabled.

Data Plane—When receiving the IP GRE encapsulated Ethernet packet, the data plane tunnel ingress processing checks the protocol field in the GRE header. If the protocol is transparent Ethernet bridging protocol (0x6558), the packet is identified as Ethernet over soft GRE packet and is directed to the Ethernet service instance classification module. The Ethernet service instance classification module classifies the packet into the service instance configured under the Virtual Ethernet interface using the VLAN tag in the packet. After the Ethernet service instance is identified, the packet goes through the programmed processing FIA under the Ethernet service instance such as vlan tag manipulation and is then sent to L2 bridge domain for further processing. At the L2 bridge domain processing module, the client source MAC address is dynamically learned, and so

is the IP GRE tunnel end-points. As a result, the MAC address table contains the IP GRE tunnel end-points for the client MAC address.

The packet is then either bridged to the external ISG for subscriber processing in the case of the two-box deployment model. In the direction where the ISG, either external or internal, sends a packet to the mobile client, the L2 bridge domain looks up the destination MAC address using the L2 bridge domain MAC address table. Once the result is found, the IP GRE tunnel end point addresses are also retrieved from the MAC address table. The L2 Ethernet packet is then encapsulated into the IP GRE tunnel using the retrieved tunnel end point address. Once encapsulated into the IP GRE packet, IP lookup is then performed and the packet is sent to the CPE.

Configuration Example: Two-box Deployment Model

```
Interface GigabitEthernet0/0/0
  description Connect-Internet-Gateway
  no ip address
  negotiation auto
  service instance 140 Ethernet
    encapsulation dot1q 140
    bridge-domain 140

Interface Virtual-Ethernet1
    description L2 EoGRE Tunnel
    arp timeout 0
    service instance 140 Ethernet
      encapsulation dot1q 140
      rewrite egress tag translate 1-to-1 dot1q 140
      bridge-domain 140
```

Additional References

Related Documents

Related Topic	Document Title
Configuration guide	*Cisco IOS Carrier Ethernet Configuration Guide*, Release 12.2SR
Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

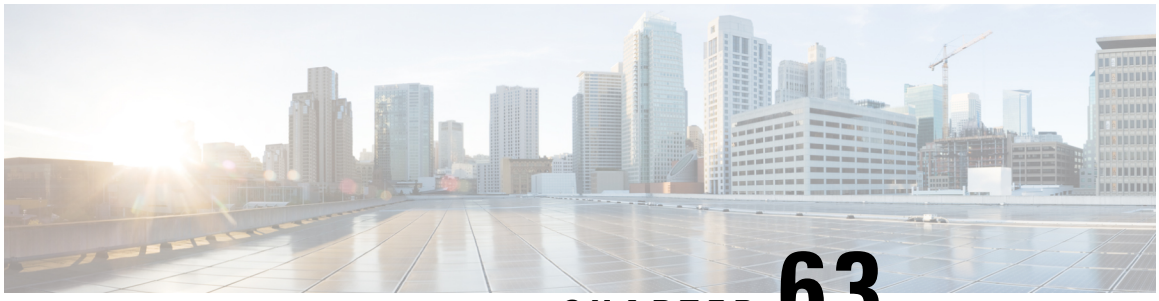
Feature Information for Layer 2 Ethernet over GRE

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 82: Feature Information for Layer 2 Ethernet over GRE

Feature Name	Releases	Feature Information
Layer 2 Ethernet over GRE	Cisco IOS XE Release 3.9S	Ethernet over Soft Generic Routing Encapsulation (EoGRE) is an aggregation solution for aggregating WiFi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic from an end host, and encapsulates the traffic in Ethernet packets over an IP GRE tunnel. The IP GRE tunnel terminates on a service provider broadband network gateway, which then terminates the end host traffic and manages the subscriber session for the end host.



CHAPTER 63

Configuring MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

The MAC Address Limiting on Service Instances, Bridge Domains, and EVC Port Channels feature addresses port security with service instances by providing the capability to control and filter MAC address learning behavior at the granularity of a per-service instance. When a violation requires a shutdown, only the customer who is assigned to a given service instance is affected and--not all customers who are using the port.

MAC address limiting is a type of MAC security and is also referred to as a MAC security component or element.

Prerequisites for MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

- An understanding of service instances and bridge domains.
- An understanding of how port channels and EtherChannels work in a network.

Restrictions for MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

- MAC address limiting for service instances and bridge domains is configured under a service instance and is permitted only after the service instance is configured under a bridge domain. If a service instance is removed from a bridge domain, all the MAC address limiting commands under it are also removed. If a bridge domain is removed from a service instance, all the MAC address limiting commands are also removed.
- The MAC Address on RSP1 port channel overlaps with the interface MAC address and the traffic is dropped from ports 1 to 8 when an interface module is placed on slot 4.
-
- System wide, the following limits apply to the total configured allowed list and learned MAC addresses:
  - Total number of MAC addresses supported under MAC Security is limited to 64K (65536).
  - Total number of secure EFPs in the system is limited to 64K (65536).
  - Total number of MAC addresses supported under MAC Security, per EFP, is limited to 1K (1024).
  - Total number of EFPs per bridge domain 4000.
  - Total number of bridge domains per system 16000.
- You can configure or remove the various MAC security elements irrespective of whether MAC security is enabled on the EFP. However, these configurations become operational only after MAC security is enabled.
- It is recommended that you enable MAC address security feature on all the EFPs in a bridge-domain.
- When you enable the MAC address security for EVC bridge domain feature, existing MAC address table entries on the EFP are removed.
- When you enable the MAC address security, the traffic is forwarded once the device learns the MAC address.
- The MAC address security for EVC bridge domain feature can be configured on an EFP only if the EFP is a member of a bridge domain.
- you can configure non-MAC address security on an EVC and enable MAC address security on a different EVC, which are in the same bridge-domain.
- If you disassociate the EFP from the BD, the MAC security feature is completely removed.
- For port-channel, this configuration is propagated to all member links in the port-channel. Consistent with the already implemented bridge domain EVC port-channel functionality, packets on a secured EFP are received on any member link, but all the egress packets are sent out to one of the selected member links.
- System does not permit addition of multicast/broadcast MAC address as a permit address. However, addition of multicast/broadcast MAC address is allowed in deny address configuration to verify such invalid packets.

- When EVC with the same EFP or service instance is created between ports 1 and 2 and MAC address m1 is configured as permit address (allowed list) on port1, the same MAC address can be configured as deny address (blocked list) on port2 and vice versa.

Information About MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

Ethernet Virtual Circuits, Service Instances, and Bridge Domains

An Ethernet virtual circuit (EVC) as defined by the Metro Ethernet Forum is a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. It is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. An EVC embodies the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a given port.

Support for Ethernet bridging is an important Layer 2 service that is offered on a router as part of an EVC. Ethernet bridging enables the association of a bridge domain with a service instance.

For information about the Metro Ethernet Forum standards, see the "Standards" table in the "Additional References" section.

EVCs on Port Channels

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links. The Ethernet Virtual Connection Services (EVCS) EtherChannel feature provides support for EtherChannels on service instances.

Note The MAC Address Security on EVC Port Channel services is supported only on bridge domains over Ethernet and is not supported on xconnect services.

EVCS uses the concepts of EVCs and service instances.

Load balancing is done on an Ethernet flow point (EFP) basis where a number of EFPs exclusively pass traffic through member links.

MAC Security and MAC Addressing

MAC security is enabled on a service instance by configuring the **mac security** command. Various MAC security elements can be configured or removed regardless of whether the **mac security** command is presently configured, but these configurations become operational only when the **mac security** command is applied.

In this document, the term "secured service instance" is used to describe a service instance on which MAC security is configured. The MAC addresses on a service instance on which MAC security is configured are referred to as "secured MAC addresses." Secured MAC addresses can be either statically configured (as a permit list) or dynamically learned.

MAC Address Permit List

A permit list is a set of MAC addresses that are permitted on a service instance. Permitted addresses permanently configured into the MAC address table of the service instance.

On a service instance that is a member of a bridge domain, the operator is permitted to configure one or more permitted MAC addresses.

For each permitted address, eligibility tests are performed and after the address passes these tests, it is either:

- Programmed into the MAC address table of the bridge domain, if MAC security is enabled on the service instance or,
- Stored in an area of memory referred to as “MAC table cache” if MAC security is not enabled on the service instance. When MAC security is enabled, the addresses from the MAC table cache are added to the MAC address table as secure addresses.

The eligibility tests performed when a user tries to add a MAC address to the permit list on a service instance are as follows:

- If the address is already a denied address on the service instance, the configuration is rejected with an appropriate error message.
- If the acceptance of this address would increase the secure address count on the service instance beyond the maximum number allowed, an attempt is made to make room by removing an existing address from the MAC address table. The only candidate for removal is a dynamically learned address on the service instance. If sufficient room cannot be made, the configuration is rejected. If the acceptance of this address would increase the secure address count on the bridge domain beyond the maximum number allowed, an attempt is made to make room by removing an existing address from the MAC address table. The only candidate for removal is a dynamically learned address on the service instance. If room cannot be made, the configuration is rejected.
- If the address is already permitted on another service instance in the same bridge domain, one of the following actions occur:
  - If the conflicting service instance has MAC security configured, the configuration is rejected with an appropriate error message.
  - If the conflicting service instance does not have MAC security configured, the configuration is accepted silently. (If the operator attempts to enable MAC security on the conflicting service instance, that attempt fails.)

MAC Address Deny List

A deny list is a set of MAC addresses that are not permitted on a service instance. An attempt to learn a denied MAC address will fail. On a service instance that is a member of a bridge domain, the operator is permitted to configure one or more denied MAC addresses. The arrival of a frame with a source MAC address that is part of a deny list will trigger a violation response.

Before a denied address can be configured, the following test is performed:

- If the address is already configured as a permitted address on the specific service instance or if the address has been learned and saved as a sticky address on the service instance, the configuration is rejected with an appropriate error message.

In all other cases, the configuration of the denied address is accepted. Typical cases include:

- The address is configured as a permitted address on another service instance in the same bridge domain, or the address has been learned and saved as a sticky address on another service instance.
- The address is present in the MAC table of the bridge domain as a dynamically learned address on the specific service instance and is deleted from the MAC table before the configuration is accepted.

MAC Address Limiting and Learning

An upper limit for the number of secured MAC addresses allowed on a bridge domain service instance can be configured. This limit includes addresses added as part of a permit list and dynamically learned MAC addresses.

Before an unknown MAC address is learned, a series of checks are run against a set of configured and operational constraints. If any of these checks fails, the address is not learned, and a configured violation response is triggered.

Static and Dynamic MAC Addresses

A static MAC address is specified as permitted on a service instance, by a **mac security permit**command. A dynamic MAC address is a source MAC address encountered by the service instance that is not present in the MAC table but is allowed into and learned by the MAC address table.

Dynamic MAC Address Learning

Dynamic MAC address learning occurs when the bridging data path encounters an ingress frame whose source address is not present in the MAC address table for the ingress secured service instance.

The MAC security component is responsible for permitting or denying the addition of the new source address into the MAC table. The following constraints apply:

- If a MAC address is to be learned, a check is performed to determine whether the number of secured MAC addresses exceed the maximum number that are permitted to be learned on the individual service instance and on the bridge domain.
- A check is performed to determine if the MAC address on an another service instance is learned on a secured service instance in the same bridge domain.
- A check is performed to verify if the new dynamic MAC address is in a deny list.

MAC Address Limiting on Service Instances

The user can configure the maximum number of MAC addresses that can exist in the MAC table that is associated with a service instance. This number includes statically configured and dynamically learned (including sticky) addresses.

On a service instance that has MAC security enabled and that does not have the maximum number of MAC addresses configured, the number of addresses allowed is one. This means that if the service instance has an associated permit list, that permit list can have only one address, and no addresses are learned dynamically. If the service instance does not have an associated permit list, one MAC address may be learned dynamically.

MAC Address Limiting for Bridge Domains

An upper limit for the number of MAC addresses that can reside in the MAC address table of a bridge domain can be set. This is set independently of the upper limit of secured MAC addresses on the service instance. An attempted violation of this bridge domain MAC address limit will cause the MAC address learn attempt to fail, and the frame to be dropped.

If the bridge domain MAC address limit is not configured, then by default, the maximum number of MAC addresses allowed on a bridge domain is the maximum number that can be supported by that platform.

Relationship Between the MAC Address Limit on a Bridge Domain and on a Service Instance

You can specify the maximum count of MAC table entries on a bridge domain and on a service instance simultaneously. However, there are no restrictions on the count that is configured on the service instance.

The table below shows an example of an initial configuration where three service instances are configured on a bridge domain:

Table 83: Bridge-Domain and Service-Instance MAC Address Limit

Bridge-Domain / Service-Instance Number	MAC Address Limit
Bridge Domain 1000	20
Service Instance 1001	5
Service Instance 1002	10
Service Instance 1003	To be configured

If you wish to configure MAC security on service instance 1003, any value can be configured for the maximum count. For example:

```
service instance 1003 ethernet
 bridge-domain 1
 mac security
 mac security maximum addresses 35
```

A MAC address limit of 35 is permitted, even though the total MAC address limit for the three service instances (5 + 10 + 35) would exceed the count (20) configured on the bridge domain. Note that during actual operation, the bridge domain limit of 20 is in effect. The dynamic secure address count cannot exceed the lowest count applicable, so it is not possible for service instance 1003 to learn 35 addresses.

MAC Move and MAC Locking

If a MAC address is present in the MAC address table for a service instance (for example, service instance 1) on which MAC security is configured, the same MAC address cannot be learned on another service instance (for example, service instance 2) in the same bridge domain.

If service instance 2 attempts to learn the same MAC address, the violation response configured on service instance 2 is triggered. If MAC security is not configured on service instance 2 and a violation response is not configured, the “shutdown” response sequence is triggered on service instance 2.

If MAC security is not enabled on service instance 1, the violation is not triggered. service instance 2 learns the MAC address and moves it from service instance 1.

For some platforms, MAC address moves are allowed but moves between secured service instances and nonsecured service instances cannot be detected.

For example, if you do not configure MAC security on service instance 2 because of a hardware limitation, a MAC move from secured service instance 1 to service instance 2 is accepted. Therefore, it is recommended that all service instances within the same bridge-domain be configured as secured service instances.

Violation Response Configuration

A violation response is a response to a MAC security violation or a failed attempt to dynamically learn a MAC address due to an address violation. MAC security violations are of two types:

Type 1 Violation --The address of the ingress frame cannot be dynamically learned due to a deny list, or because doing so would cause the maximum number of secure addresses to be exceeded .

Type 2 Violation --The address of the ingress frame cannot be dynamically learned because it is already "present" on another secured service instance .

There are three possible sets of actions that can be taken in response to a violation:

1. **Shutdown**
   - The ingress frame is dropped.
   - The service instance on which the offending frame arrived is shut down.
   - The event and the response are logged to SYSLOG.
2. **Restrict**
   - The ingress frame is dropped.
   - The event and the response are logged to SYSLOG.
3. **Protect**
   - The ingress frame is dropped.

Note The ingress frame is dropped silently, without sending any violation report to the SYSLOG.

If a violation response is not configured, the default response mode is shutdown. The violation response can be configured to protect or restrict mode. A "no" form of a violation response, sets the violation response to the default mode of shutdown.

You are allowed to configure the desired response for a Type 1 and Type 2 violations on a service instance. For a Type 1 violation on a bridge domain (that is, if the learn attempt conforms to the policy configured on the service instance, but violates the policy configured on the bridge domain), the response is always "Protect." This is not configurable.

In Restrict mode, the violation report is sent to SYSLOG at level LOG_WARNING.

Support for the different types of violation responses depends on the capabilities of the platform. The desired violation response can be configured on the service instance. The configured violation response does not take effect unless and until MAC security is enabled using the **mac security** command.

MAC Address Aging Configuration

A specific time scheduler can be set to age out secured MAC addresses that are dynamically learned or statically configured on both service instances and bridge domains, thus freeing up unused addresses from the MAC address table for other active subscribers.

The set of rules applied to age out secured MAC addresses is called secure aging. By default, the entries in the MAC address table of a secured service instance are never aged out. This includes permitted addresses and dynamically learned addresses.

The **mac security aging time** *aging-time* command sets the aging time of the addresses in the MAC address table to <*n* > minutes. By default, this affects only dynamically learned (not including sticky) addresses--permitted addresses and sticky addresses are not affected by the application of this command.

By default, the aging time <n> configured via the **mac security aging time** *aging-time* command is an absolute time. That is, the age of the MAC address is measured from the instant that it was first encountered on the service instance. This interpretation can be modified by using the **mac security aging time** *aging-time* **inactivity** command, which specifies that the age <n> be measured from the instant that the MAC address was last encountered on the service instance.

The **mac security aging static**and **mac security aging sticky** commands specify that the **mac security aging time**aging-time command must be applicable to permitted and sticky MAC addresses, respectively. In the case of permitted MAC addresses, the absolute aging time is measured from the time the address is entered into the MAC address table (for example, when it is configured or whenever the **mac security** command is entered--whichever is later).

If the **mac security aging time** command is not configured, the **mac security aging static** command has no effect.

Sticky MAC Address Configurations

The ability to make dynamically learned MAC addresses on secured service instances permanent even after interface transitions or device reloads can be set up and configured. A dynamically learned MAC address that is made permanent on a secured service instance is called a “sticky MAC address”. The **mac security sticky** command is used to enable the sticky MAC addressing feature on a service instance.

With the “sticky” feature enabled on a secured service instance, MAC addresses learned dynamically on the service instance are kept persistent across service instance line transitions and device reloads.

The sticky feature has no effect on statically configured MAC addresses. The sticky addresses are saved in the running configuration. Before the device is reloaded, it is the responsibility of the user to save the running configuration to the startup configuration. Doing this will ensure that when the device comes on, all the MAC addresses learned dynamically previously are immediately populated into the MAC address table.

The **mac security sticky address** *mac-address* command can configure a specific MAC address as a sticky MAC address. The use of this command is not recommended for the user because configuring a MAC address as a static address does the same thing. When sticky MAC addressing is enabled by the **mac security sticky** command, the dynamically learned addresses are marked as sticky and a **mac security sticky address** *mac-address* command is automatically generated and saved in the running configuration for each learned MAC address on the service instances.

Aging for Sticky Addresses

MAC addresses learned on a service instance that has the sticky behavior enabled are subject to aging as configured by the **mac security aging time** and **mac security aging sticky** commands. In other words, for the purpose of aging functionality, sticky addresses are treated the same as dynamically learned addresses.

Transitions

This section contains a description of the expected behavior of the different MAC security elements when various triggers are applied; for example, configuration changes or link state transitions.

MAC Security Enabled on a Service Instance

When MAC security is enabled on a service instance, all existing MAC table entries for the service instance are purged. Then, permitted MAC address entries and sticky addresses are added to the MAC table, subject to the prevailing MAC address limiting constraints on the bridge domain.

If MAC address limits are exceeded, any MAC address that fails to get added is reported via an error message to the console, the attempt to enable MAC security on the service instance fails, and the already added permitted entries are backed out or removed.

The aging timer for all entries is updated according to the secure aging rules.

MAC Security Disabled on a Service Instance

The existing MAC address table entries for this service instance are purged.

Service Instance Moved to a New Bridge Domain

This transition sequence applies to all service instances, whether or not they have MAC security configured. All the MAC addresses on this service instance in the MAC address table of the old bridge domain are removed. The count of dynamically learned addresses in the old bridge domain is decremented. Then, all the MAC security commands are permanently erased from the service instance.

Service Instance Removed from a Bridge Domain

All the MAC addresses in the MAC address table that attributable to this service instance are removed, and the count of dynamically learned addresses in the bridge domain is decremented. Since MAC security is applicable only on service instances that are members of a bridge domain, removing a service instance from a bridge domain causes all the MAC security commands to be erased permanently.

Service Instance Shut Down Due to Violation

All dynamically learned MAC addresses in the MAC address table are removed, and all the other MAC security state values are left unchanged. The only change is that no traffic is forwarded, and therefore no learning can take place.

Interface Service Instance Down Linecard OIR Removed

The MAC tables of all the affected bridge domains are cleared of all the entries attributable to the service instances that are down.

Interface Service Instance Re-activated Linecard OIR Inserted

The static and sticky address entries in the MAC tables of the affected bridge domains are re-created to the service instances that are activated.

MAC Address Limit Decreased

When the value of the MAC address limit on the service instance is changed initially, a sanity check is performed to ensure that the new value of <n> is greater than or equal to the number of permitted entries. If not, the command is rejected. The MAC table is scanned for addresses that are attributable to this service instance, and dynamically learned MAC addresses are removed when the new MAC address limit is less than the old MAC address limit.

Sticky Addresses Added or Removed on a Service Instance

Existing dynamically learned MAC addresses remain unchanged. All new addresses learned become “sticky” addresses.

Disabling sticky addresses causes all sticky secure MAC addresses on the service instance to be removed from the MAC address table. All new addresses learned become dynamic addresses on the service instance and are subject to aging.

How to Configure MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

Enabling MAC Security on a Service Instance

Perform this task to enable MAC address security on a service instance.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

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** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 8 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Enabling MAC Security on an EVC Port Channel

Before you begin

Note

- Bridge-domain, xconnect, and Ethernet virtual circuits (EVCs) are allowed only over the port channel interface and the main interface.
- If you configure a physical port as part of a channel group, you cannot configure EVCs under that physical port.

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** *channel-group*

Example:

```
Device(config)# interface port-channel 2
```

Specifies the port channel group number and enters interface configuration mode.

- Acceptable values are integers from 1 to 64.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

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** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 8 end

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Configuring a MAC Address Permit List

Perform this task to configure permitted MAC addresses on a service instance that is a member of a bridge domain.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

Defines the matching criteria to be used for mapping ingress dot1q frames on an interface to the appropriate service instance.

Step 6 **bridge-domain** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security address permit** *mac-address*

Example:

```
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
```

Adds the specified MAC address as a permit MAC address for the service instance.

Step 8 **mac security address permit** *mac-address*

Example:

```
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaab
```

Adds the specified MAC address as a permitted MAC address for the service instance.

Step 9 **mac security address permit** *mac-address*

Example:

```
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaac
```

Adds the specified MAC address as a permitted MAC address for the service instance.

Step 10 **mac security address permit** *mac-address*

Example:

```
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaad
```

Adds the specified MAC address as a permitted MAC address for the service instance.

Step 11 **mac security address permit** *mac-address*

Example:

```
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaae
```

Adds the specified MAC address as a permitted MAC address for the service instance.

Step 12 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 13 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Configuring a MAC Address Deny List

Perform this task to configure a list of MAC addresses that are not allowed on a service instance that is a member of a bridge domain.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

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** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security address deny** *mac-address*

Example:

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaaa
```

Adds the specified MAC address as a denied MAC address for the service instance.

Step 8 **mac security address deny** *mac-address*

Example:

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaab
```

Adds the specified MAC address as a denied MAC address for the service instance.

Step 9 **mac security address deny** *mac-address*

Example:

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaac
```

Adds the specified MAC address as a denied MAC address for the service instance.

Step 10 **mac security address deny** *mac-address*

Example:

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaad
```

Adds the specified MAC address as a denied MAC address for the service instance.

Step 11 **mac security address deny** *mac-address*

Example:

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaae
```

Adds the specified MAC address as a denied MAC address for the service instance.

Step 12 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 13 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Configuring MAC Address Limiting on a Bridge Domain

Perform this task to configure an upper limit for the number of secured MAC addresses that reside in a bridge domain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **mac limit maximum addresses** *maximum-addresses*
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	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 100`	Configures components on a bridge domain and enters bridge-domain configuration mode.

	Command or Action	Purpose
Step 4	**mac limit maximum addresses** *maximum-addresses* **Example:** `Device(config-bdomain)# mac limit maximum addresses 200`	Sets the MAC limit maximum addresses.
Step 5	end **Example:** `Device(config-bdomain)# end`	Returns to user EXEC mode.

Configuring MAC Address Limiting on a Service Instance

Perform this task to configure an upper limit for the number of secured MAC addresses allowed on a service instance. This number includes addresses added as part of a permit list as well as dynamically learned MAC addresses. If the upper limit is decreased, all learned MAC entries are removed. If the upper limit is decreased, one or more learned MAC entries may be removed. The EFP secure MAC address limitation range is [1-1024], so the maximum is 1024.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security maximum addresses**
8. **mac security**
9. **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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Device(config-if)# service instance 100 ethernet`	Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 200`	Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.
Step 7	**mac security maximum addresses** **Example:** `Device(config-if-srv)# mac security maximum addresses 500`	Sets the maximum number of secure addresses permitted on the service instance.
Step 8	**mac security** **Example:** `Device(config-if-srv)# mac security`	Enables MAC security on the service instance.
Step 9	**end** **Example:** `Device(config-if-srv)# end`	Returns to user EXEC mode.

Configuring a MAC Address Violation

Perform this task to specify the expected behavior of a device when an attempt to dynamically learn a MAC address fails because the configured MAC security policy on the service instance was violated.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.

Step 6 **bridge-domain** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 100
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 Do one of the following:

- **mac security violation restrict**
- **mac security violation protect**

Example:

```
Device(config-if-srv)# mac security violation restrict
```

Example:

```
Device(config-if-srv)# mac security violation protect
```

Sets the violation mode (for Type 1 and 2 violations) to restrict.

or

Sets the violation mode (for Type 1 and 2 violations) to protect.

- If a MAC security violation response is not specified, by default, the violation mode is shutdown.

Step 8 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 9 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Configuring MAC Address Aging

Perform this task to configure the aging of secured MAC addresses under MAC security. Secured MAC addresses are not subject to the normal aging of MAC table entries. If aging is not configured, secured MAC addresses are never aged out.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

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** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security aging time** *aging-time* **[inactivity]**

Example:

```
Device(config-if-srv)# mac security aging time 200 inactivity
```

Sets the aging time for secure addresses, in minutes. The optional **inactivity** keyword specifies that the aging out of addresses is based on inactivity of the sending hosts (as opposed to absolute aging).

Step 8 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 9 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Configuring a Sticky MAC Address

If sticky MAC addressing is configured on a secured service instance, MAC addresses that are learned dynamically on the service instance are retained during a link-down condition. Perform this task to configure sticky MAC addresses on a service instance.

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** *type number*

Example:

```
Device(config)# interface gigabitethernet2/0/1
```

Specifies the interface type and number, and enters interface configuration mode.

Step 4 **service instance** *id* **ethernet**

Example:

```
Device(config-if)# service instance 100 ethernet
```

Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.

Step 5 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 100
```

Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.

Step 6 **bridge-domain** *bridge-id*

Example:

```
Device(config-if-srv)# bridge-domain 200
```

Binds the service instance to a bridge- domain instance where *bridge-id* is the identifier for the bridge- domain instance.

Step 7 **mac security sticky address** *mac-address*

Example:

```
Device(config-if-srv)# mac security sticky address 1111.2222.3333
```

Sets up a MAC address to be declared as a sticky MAC address on the service instance.

Step 8 **mac security**

Example:

```
Device(config-if-srv)# mac security
```

Enables MAC security on the service instance.

Step 9 **end**

Example:

```
Device(config-if-srv)# end
```

Returns to user EXEC mode.

Displaying the MAC Security Status of a Specific Service Instance

Perform this task to display the MAC security status of a service instance.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance id** *id* **interface** *type* *number* **mac security**

Example:

```
Device# show ethernet service instance id 100 interface gigabitethernet1/1 mac security
```

Displays the MAC security status of a specific service instance.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Displaying the Service Instances with MAC Security Enabled

Perform this task to display all the service instances with MAC security enabled.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance mac security**

Example:

```
Device# show ethernet service instance mac security
```

Displays all the service instances with MAC security enabled.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Displaying the Service Instances with MAC Security Enabled on a Specific Bridge Domain

Perform this task to display the service instances on a specific bridge domain that have MAC security enabled.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show bridge-domain** *id* **mac security**

Example:

```
Device# show bridge-domain 100 mac security
```

Displays all the service instances with MAC security enabled on a specific bridge domain.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the MAC Addresses of All Secured Service Instances

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance mac security address**

Example:

```
Device# show ethernet service instance mac security address
```

Displays the secured addresses on all the service instances.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the MAC Addresses of a Specific Service Instance

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance id** *id* **interface** *type number* **mac security address**

Example:

```
Device# show ethernet service instance id 200 interface GigabitEthernet 1/0 mac security address
```

Displays the addresses of a specific service instance.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the MAC Addresses of All Service Instances on a Specific Bridge Domain

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show bridge-domain** *id* **mac security address**

Example:

```
Device# show bridge-domain 100 mac security address
```

Displays the secured addresses of all the service instances on a specified bridge domain.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the MAC Security Statistics of a Specific Service Instance

This section describes how to display the MAC security statistics of a specific service instance.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet service instance id** *id* **interface** *type number* **mac security statistics**

Example:

```
Device# show ethernet service instance id 100 interface gigabitethernet1/1 mac security statistics
```

Displays the MAC security statistics of a specific service instance.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the MAC Security Statistics of All Service Instances on a Specific Bridge Domain

Perform this task to display the MAC security statistics of all the service instances on a specific bridge domain.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show bridge-domain** *bridge-id* **mac security statistics**

Example:

```
Device# show bridge-domain 100 mac security statistics
```

Displays the MAC security statistics of all service instances that belong to a specific bridge domain.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Showing the Last Violation Recorded on Each Service Instance on a Specific Bridge Domain

Perform this task to display the last violation recorded on each service instance on a specific bridge domain. Service instances on which there have been no violations are excluded from the output.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show bridge-domain** *bridge-id* **mac security last violation**

Example:

```
Device# show bridge-domain 100 mac security last violation
```

Displays information about the last violation recorded on each of the service instances that belong to the bridge domain.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Clearing All Dynamically Learned Secure MAC Addresses on a Service Instance

Perform this task to clear all dynamically learned Secure MAC addresses on a service instance.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **clear ethernet service instance id** *id* **interface** *type number* **mac table**

Example:

```
Device# clear ethernet service instance id 100 interface gigabitethernet0/0/1 mac table
```

Clears all the dynamically learned Secure MAC addresses on the specified service instance.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Clearing All Dynamically Learned MAC Addresses on a Bridge Domain

Perform this task to clear all dynamically learned MAC addresses on a bridge domain.

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **clear bridge-domain** *bridge-id* **mac table**

Example:

```
Device# clear bridge-domain 100 mac table
```

Clears all dynamically learned MAC addresses on the specified bridge domain.

Step 3 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Bringing a Specific Service Instance Out of the Error-Disabled State

Perform this task to bring a specific service instance out of the error-disabled state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **bridge-domain** *bridge-id*
7. **mac security**
8. **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** *type number* **Example:** `Device(config)# interface gigabitethernet2/0/1`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Device(config-if)# service instance 100 ethernet`	Creates a service instance (an instance of an EVC) on an interface and enters service instance configuration mode.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 100`	Defines the matching criteria to be used to map ingress dot1q frames on an interface to the appropriate service instance.
Step 6	**bridge-domain** *bridge-id* **Example:** `Device(config-if-srv)# bridge-domain 200`	Binds the service instance to a bridge-domain instance where *bridge-id* is the identifier for the bridge-domain instance.
Step 7	**mac security** **Example:** `Device(config-if-srv)# mac security`	Enables MAC security on the service instance.
Step 8	**end** **Example:**	Returns to user EXEC mode.

	Command or Action	Purpose
	`Device(config-if-srv)# end`	

Configuration Examples for MAC Address Limiting on Service Instances and Bridge Domains and EVC Port Channels

Example Enabling MAC Security on a Service Instance

The following example shows how to enable MAC security on a service instance:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Enabling MAC Security on an EVC Port Channel

The following example shows how to enable MAC Security on an EVC port channel:

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Configuring a MAC Address Permit List

The following example shows how to configure a MAC address permit list:

Example Configuring a MAC Address Deny List

The following example shows how to configure a MAC address deny list:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaaa
```

```
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaab
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaac
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaad
Device(config-if-srv)# mac security address deny a2aa.aaaa.aaae
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Configuring MAC Address Limiting on a Bridge Domain

```
Device> enable
Device# configure terminal
Device(config)# bridge-domain 100
Device(config-bdomain)# mac limit maximum addresses 1000
Device(config-bdomain)# end
```

Example Configuring a MAC Address Limit on a Service Instance

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security maximum addresses 10
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Configuring a MAC Address Violation Response

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security address permit a2aa.aaaa.aaaa
Device(config-if-srv)# mac security violation protect
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Configuring MAC Address Aging

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 4/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security aging time 10
Device(config-if-srv)# mac security
Device(config-if-srv)# end
```

Example Configuring a Sticky MAC Address

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 3/0/1
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1Q 100
Device(config-if-srv)# bridge-domain 100
Device(config-if-srv)# mac security sticky address 1111.2222.3333
Device(config-if-srv)# mac security
```

Additional References

Related Documents

Related Topic	Document Title
CFM commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
Configuring Ethernet connectivity fault management in a service provider network (Cisco pre-Standard CFM Draft 1)	"Configuring Ethernet Connectivity Fault Management in a Service Provider Network" module in the *Cisco IOS Carrier Ethernet Configuration Guide*
Ethernet Local Management Interface on a provider edge device	"Configuring Ethernet Local Management Interface on a Provider Edge Device" module in the *Cisco IOS Carrier Ethernet Configuration Guide*
IP SLAs for Metro Ethernet	"IP SLAs for Metro Ethernet"
NSF/SSO and MPLS	"NSF/SSO - MPLS LDP and LDP Graceful Restart"
ISSU feature and functions	"Cisco IOS Broadband High Availability In Service Software Upgrade"
Performing an ISSU	"Cisco IOS In Service Software Upgrade Process and Enhanced Fast Software Upgrade Process"
SSO	"Stateful Switchover" chapter of the *Cisco IOS High Availability Configuration Guide*

Standards

Standard	Title
IEEE 802.1ag Standard	*802.1ag - Connectivity Fault Management*
IEEE 802.3ah	*IEEE 802.3ah Ethernet in the First Mile*
IETF VPLS OAM	*L2VPN OAM Requirements and Framework*

Standard	Title
ITU-T	ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks

MIBs

MIB	MIBs Link
CISCO-ETHER-CFM-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

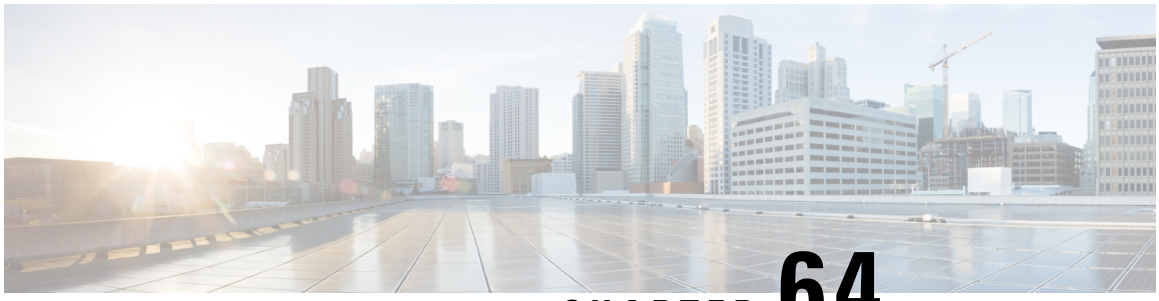
Feature Information for MAC Address Limiting on Service Instances Bridge Domains and EVC Port Channels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 84: Feature Information for MAC Address Limiting on Service Instances, Bridge Domains, and EVC Port Channels

Feature Name	Releases	Feature Information
MAC Address Limiting on Service Instances and Bridge Domains	Cisco IOS XE 3.7S Cisco IOS XE Gibraltar 16.11.a	The MAC Address Limiting on Service Instances and Bridge Domains feature addresses port security with service instances by providing the capability to control and filter MAC address learning behavior at the granularity of a per-service instance. When a violation requires a shutdown, only the customer that is assigned to a given service instance is affected. MAC address limiting is a type of MAC security and is also referred to as a MAC security component or element. The following commands were introduced or modified: **bridge-domain (global)**, **bridge-domain (service instance)**, **clear bridge-domain mac-table**, **clear ethernet service instance**, **errdisable recovery cause mac-security**, **interface**, **mac limit maximum addresses**,**mac security**,**show bridge-domain**, **show ethernet service instance**. Support was added in Cisco IOS XE Gibraltar 16.11.a for Cisco ASR 1000 Series Aggregation Services Routers, Cisco Cloud Services Router 1000v, and Cisco 4000 Series Integrated Services Routers.



CHAPTER 64

Configuring Ethernet Local Management Interface at a Provider Edge

The advent of Ethernet as a metropolitan-area network (MAN) and WAN technology imposes a new set of Operation, Administration, and Management (OAM) requirements on Ethernet's traditional operations, which had centered on enterprise networks only. The expansion of Ethernet technology into the domain of service providers, where networks are substantially larger and more complex than enterprise networks and the user-base is wider, makes operational management of link uptime crucial. More importantly, the timeliness in isolating and responding to a failure becomes mandatory for normal day-to-day operations, and OAM translates directly to the competitiveness of the service provider.

The “Configuring Ethernet Local Management Interface at a Provide Edge” module provides general information about configuring an Ethernet Local Management Interface (LMI), an OAM protocol, on a provider edge (PE) device.

Prerequisites for Configuring Ethernet Local Management Interface at a Provider Edge

- Ethernet Operation, Administration, and Management (OAM) must be operational in the network.
- For Ethernet OAM to operate, the provider edge (PE) side of a connection must be running Ethernet Connectivity Fault Management (CFM) and Ethernet Local Management Interface (LMI).
- All VLANs used on a PE device to connect to a customer edge (CE) device must also be created on that CE device.

- To use nonstop forwarding (NSF) and In Service Software Upgrade (ISSU), stateful switchover (SSO) must be configured and working properly.

Restrictions for Configuring Ethernet Local Management Interface at a Provider Edge

- Ethernet Local Management Interface (LMI) is not supported on routed ports, EtherChannel port channels, ports that belong to an EtherChannel, private VLAN ports, IEEE 802.1Q tunnel ports, Ethernet over Multiprotocol Label Switching (MPLS) ports, or Ethernet Flow Points (EFPs) on trunk ports.
- Ethernet LMI cannot be configured on VLAN interfaces.

Information About Configuring Ethernet Local Management Interface at a Provider Edge

Ethernet Virtual Circuits Overview

An Ethernet virtual circuit (EVC) as defined by the Metro Ethernet Forum is a port level point-to-point or multipoint-to-multipoint Layer 2 circuit. EVC status can be used by a customer edge (CE) device to find an alternative path in to the service provider network or in some cases to fall back to a backup path over Ethernet or another alternative service such as ATM.

Ethernet LMI Overview

Ethernet Local Management Interface (LMI) is an Ethernet Operation, Administration, and Management (OAM) protocol between a customer edge (CE) device and a provider edge (PE) device. Ethernet LMI provides CE devices with the status of Ethernet virtual circuits (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs and provides information that enables CE devices to autoconfigure. Specifically, Ethernet LMI runs on the PE-CE User-Network Interface (UNI) link and notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC.

Ethernet LMI interoperates with Ethernet Connectivity Fault Management (CFM), an OAM protocol that runs within the provider network to collect OAM status. Ethernet CFM runs at the provider maintenance level (user provider edge [UPE] to UPE at the UNI). Ethernet LMI relies on the OAM Ethernet Infrastructure (EI) to interwork with CFM to learn the end-to-end status of EVCs across CFM domains.

Ethernet LMI is disabled globally by default. When Ethernet LMI is enabled globally, all interfaces are automatically enabled. Ethernet LMI can also be enabled or disabled at the interface to override the global configuration. The last Ethernet LMI command issued is the command that has precedence. No EVCs, Ethernet service instances, or UNIs are defined, and the UNI bundling service is bundling with multiplexing.

Ethernet CFM Overview

Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance (per VLAN) Ethernet layer Operation, Administration, and Management (OAM) protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end CFM can be from provider edge (PE) device to PE device or from customer edge (CE) device to CE device. For more information about Ethernet CFM, see "Configuring Ethernet Connectivity Fault Management in a Service Provider Network" in the *Carrier Ethernet Configuration Guide*.

OAM Manager Overview

The OAM manager is an infrastructure element that streamlines interaction between Operation, Administration, and Management (OAM) protocols. The OAM manager requires two interworking OAM protocols, Ethernet Connectivity Fault Management (CFM) and Ethernet Local Management Interface (LMI). No interactions are required between Ethernet LMI and the OAM manager on the customer edge (CE) side. On the User Provider-Edge (UPE) side, the OAM manager defines an abstraction layer that relays data collected from Ethernet CFM to the Ethernet LMI device.

Ethernet LMI and the OAM manager interaction is unidirectional, from the OAM manager to Ethernet LMI on the UPE side of the device. An information exchange results from an Ethernet LMI request or is triggered by the OAM manager when it receives notification from the OAM protocol that the number of UNIs has changed. A change in the number of UNIs may cause a change in Ethernet virtual circuit (EVC) status.

The OAM manager calculates EVC status given the number of active user network interfaces (UNIs) and the total number of associated UNIs. You must configure CFM to notify the OAM manager of all changes to the number of active UNIs or to the remote UNI ID for a given service provider VLAN (S-VLAN) domain.

The information exchanged is as follows:

- EVC name and availability status (active, inactive, partially active, or not defined)
- Remote UNI name and status (up, disconnected, administratively down, excessive frame check sequence [FCS] failures, or not reachable)
- Remote UNI counts (the total number of expected UNIs and the number of active UNIs)

Benefits of Ethernet LMI at a Provider Edge

- Communication of end-to-end status of the Ethernet virtual circuit (EVC) to the customer edge (CE) device
- Communication of EVC and user network interface (UNI) attributes to a CE device
- Competitive advantage for service providers

HA Features Supported by Ethernet LMI

In access and service provider networks using Ethernet technology, high availability (HA) is a requirement, especially on Ethernet operations, administration, and management (OAM) components that manage Ethernet virtual circuit (EVC) connectivity. End-to-end connectivity status information is critical and must be maintained on a hot standby Route Processor (RP) (a standby RP that has the same software image as the active RP and

supports synchronization of line card, protocol, and application state information between RPs for supported features and protocols).

End-to-end connectivity status is maintained on the customer edge (CE), provider edge (PE), and access aggregation PE (uPE) network nodes based on information received by protocols such as Ethernet Local Management Interface (LMI), Connectivity Fault Managment (CFM), and 802.3ah. This status information is used to either stop traffic or switch to backup paths when an EVC is down.

Metro Ethernet clients (E-LMI, CFM, 802.3ah) maintain configuration data and dynamic data, which is learned through protocols. Every transaction involves either accessing or updating data in the various databases. If the database is synchronized across active and standby modules, the modules are transparent to clients.

The Cisco infrastructure provides component application programming interfaces (APIs) that are helpful in maintaining a hot standby RP. Metro Ethernet HA clients (E-LMI, HA/ISSU, CFM HA/ISSU, 802.3ah HA/ISSU) interact with these components, update the database, and trigger necessary events to other components.

Benefits of Ethernet LMI HA

- Elimination of network downtime for Cisco software image upgrades, resulting in higher availability.
- Elimination of resource scheduling challenges associated with planned outages and late night maintenance windows
- Accelerated deployment of new services and applications and faster implementation of new features, hardware, and fixes due to the elimination of network downtime during upgrades
- Reduced operating costs due to outages while the system delivers higher service levels due to the elimination of network downtime during upgrades

NSF SSO Support in Ethernet LMI

The redundancy configurations stateful switchover (SSO) and nonstop forwarding (NSF) are supported in Ethernet Local Management Interface (LMI) and are automatically enabled. A switchover from an active to a standby Route Processor (RP) or a standby Route Switch Processor (RSP) occurs when the active RP or RSP fails, is removed from the networking device, or is manually taken down for maintenance. The primary function of Cisco NSF is to continue forwarding IP packets following an RP or RSP switchover. NSF also interoperates with the SSO feature to minimize network downtime following a switchover.

For detailed information about the SSO and NSF features, see the *High Availability Configuration Guide*.

ISSU Support in Ethernet LMI

In Service Software Upgrade (ISSU) allows you to perform a Cisco software upgrade or downgrade without disrupting packet flow. Ethernet Local Management Interface (LMI) performs updates of the parameters within the Ethernet LMI database to the standby route processor (RP) or standby route switch processor (RSP). This checkpoint data requires ISSU capability to transform messages from one release to another. All the components that perform active processor to standby processor updates using messages require ISSU support. ISSU is automatically enabled in Ethernet LMI.

ISSU lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. For detailed information about ISSU, see the *High Availability Configuration Guide*.

How to Configure Ethernet Local Management Interface at a Provider Edge

Configuring Ethernet LMI Interaction with CFM

For Ethernet Local Management Interface (LMI) to function with Connectivity Fault Management (CFM), you must configure Ethernet virtual circuits (EVCs), Ethernet service instances including untagged Ethernet flow points (EFPs), and Ethernet LMI customer VLAN mapping. Most of the configuration occurs on the provider edge (PE) device on the interfaces connected to the customer edge (CE) device. On the CE device, you need only enable Ethernet LMI on the connecting interface. Also, you must configure operations, administration, and management (OAM) parameters; for example, EVC definitions on PE devices on both sides of a metro network.

CFM and OAM interworking requires an inward facing Maintenance Entity Group End Point (MEP).

Configuring the OAM Manager

Note If you configure, change, or remove a user network interface (UNI) service type, Ethernet virtual circuit (EVC), Ethernet service instance, or customer edge (CE)-VLAN configuration, all configurations are checked to ensure that the configurations match (UNI service type with EVC or Ethernet service instance and CE-VLAN configuration). The configuration is rejected if the configurations do not match.

Perform this task to configure the OAM manager on a provider edge (PE) device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id*
4. **service** *csi-id* **evc** *evc-name* **vlan** *vlan-id*
5. **continuity-check**
6. **continuity-check interval** *time*
7. **exit**
8. **exit**
9. **ethernet evc** *evc-id*
10. **oam protocol** {**cfm domain** *domain-name* | **ldp**}
11. **uni count** *value* [**multipoint**]
12. **exit**
13. Repeat Steps 3 through 12 to define other CFM domains that you want OAM manager to monitor.
14. **interface** *type number*
15. **service instance** *id* **ethernet** [*evc-id*]
16. **ethernet lmi ce-vlan map** {*vlan-id* [**untagged**] | **any** | **default** | **untagged**}
17. **ethernet lmi interface**

18. **encapsulation dot1q** *vlan-id*
19. **bridge-domain** *domain-number*
20. **cfm mep domain** *domain-name* **mpid** *mpid-id*
21. **exit**
22. **service instance** *service-instance-id* **ethernet**
23. **encapsulation untagged**
24. **l2protocol peer**
25. **bridge-domain** *bridge-domain-number*
26. **exit**
27. **ethernet uni** [**bundle** [**all-to-one**] | **id** *uni-id* | **multiplex**]
28. **end**

DETAILED STEPS

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 **ethernet cfm domain** *domain-name* **level** *level-id*

Example:

```
Device(config)# ethernet cfm domain cstmr1 level 3
```

Defines a Connectivity Fault Management (CFM) domain, sets the domain leve,l and enters Ethernet CFM configuration mode.

Step 4 **service** *csi-id* **evc** *evc-name* **vlan** *vlan-id*

Example:

```
Device(config-ecfm)# service csi2 evc evc_1 vlan 10
```

Defines a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain, and enters Ethernet CFM service configuration mode.

Step 5 **continuity-check**

Example:

```
Device(config-ecfm-srv)# continuity-check
```

Enables the transmission of continuity check messages (CCMs).

Step 6 **continuity-check interval** *time*

Example:

```
Device(config-ecfm-srv)# continuity-check interval 1s/10s/1m/10m
```

Enables the transmission of continuity check messages (CCMs) at specific intervals.

Step 7 **exit**

Example:

```
Device(config-ecfm-srv)# exit
```

Returns to Ethernet CFM configuration mode.

Step 8 **exit**

Example:

```
Device(config-ecfm)# exit
```

Returns to global configuration mode.

Step 9 **ethernet evc** *evc-id*

Example:

```
Device(config)# ethernet evc 50
```

Defines an EVC and enters EVC configuration mode.

Step 10 **oam protocol** {**cfm domain** *domain-name* | **ldp**}

Example:

```
Device(config-evc)# oam protocol cfm domain cstmr1
```

Configures the Ethernet virtual circuit (EVC) operations, administration, and management (OAM) protocol as CFM for the CFM domain maintenance level as configured in Steps 3 and 4.

Note If the CFM domain does not exist, this command is rejected, and an error message is displayed.

Step 11 **uni count** *value* [**multipoint**]

Example:

```
Device(config-evc)# uni count 3
```

(Optional) Sets the User Network Interface (UNI) count for the EVC.

- If this command is not issued, the service defaults to a point-to-point service. If a value of 2 is entered, point-to-multipoint service becomes an option. If a value of 3 or greater is entered, the service is point-to-multipoint.

Note If you enter a number greater than the number of endpoints, the UNI status is partially active even if all endpoints are up. If you enter a UNI count less than the number of endpoints, status might be active, even if all endpoints are not up.

Step 12 **exit**

Example:

```
Device(config-evc)# exit
```

Returns to global configuration mode.

Step 13 Repeat Steps 3 through 12 to define other CFM domains that you want OAM manager to monitor.

Example:

–

Step 14 **interface** *type number*

Example:

Specifies a physical interface connected to the CE device and enters interface configuration mode.

Step 15 **service instance** *id* **ethernet** [*evc-id*]

Example:

```
Device(config-if)# service instance 400 ethernet 50
```

Configures an Ethernet service instance on the interface and enters Ethernet service configuration mode.

- The Ethernet service instance identifier is a per-interface service identifier and does not map to a VLAN.

Step 16 **ethernet lmi ce-vlan map** {*vlan-id* [**untagged**] | **any** | **default** | **untagged**}

Example:

```
Device(config-if-srv)# ethernet lmi ce-vlan map 30
```

Configures an Ethernet LMI customer VLAN-to-EVC map for a particular UNI.

Note To specify both VLAN IDs and untagged VLANs in the map, specify the VLAN IDs first and then specify the **untagged** keyword as follows: **ethernet lmi ce-vlan map 100,200,300,untagged**. Also, if the **untagged** keyword is not specified in the map configuration, the main interface line protocol on the Customer Edge (CE) device will be down.

Step 17 **ethernet lmi interface**

Example:

```
Device(config-if-srv)# ethernet lmi interface
```

Enables Ethernet local management interface (LMI) on a UNI.

Step 18 **encapsulation dot1q** *vlan-id*

Example:

```
Device(config-if-srv)# encapsulation dot1q 2
```

Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

Step 19 **bridge-domain** *domain-number*

Example:

```
Device(config-if-srv)# bridge-domain 1
```

Binds a service instance to a bridge domain instance.

Step 20 **cfm mep domain** *domain-name* **mpid** *mpid-id*

Example:

```
Device(config-if-srv)# cfm mep domain provider mpid 10
```

Configures a maintenance endpoint (MEP) for a domain.

Step 21 **exit**

Example:

```
Device(config-if-srv)# exit
```

Returns to interface configuration mode.

Step 22 **service instance** *service-instance-id* **ethernet**

Example:

```
Device(config-if)# service instance 22 ethernet
```

Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.

Step 23 **encapsulation untagged**

Example:

```
Device(config-if-srv)# encapsulation untagged
```

Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

Step 24 **l2protocol peer**

Example:

```
Device(config-if-srv)# l2protocol peer
```

Configures transparent Layer 2 protocol peering on the interface.

Step 25 **bridge-domain** *bridge-domain-number*

Example:

```
Device(config-if-srv)# bridge-domain 1
```

Binds a service instance to a bridge domain instance.

Step 26 **exit**

Example:

```
Device(config-if)# exit
```

Returns to interface configuration mode.

Step 27 **ethernet uni** [**bundle** [**all-to-one**] | **id** *uni-id* | **multiplex**]

Example:

```
Device(config-if)# ethernet uni bundle
```

Sets UNI bundling attributes.

Step 28 **end**

Example:

```
Device(config-if)# end
```

Returns to privileged EXEC mode.

Enabling Ethernet LMI

The order in which the global and interface configuration commands are issued determines the configuration. The last command that is issued has precedence.

Perform this task to enable Ethernet Local Management Interface (LMI) on a device or on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ethernet lmi interface**
5. **ethernet lmi** {**n393** *value* | **t392** *value*}
6. **end**

DETAILED STEPS

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** *type number*

Example:

```
Device(config)# interface ethernet 1/3
```

Defines an interface to configure as an Ethernet LMI interface and enters interface configuration mode.

Step 4 **ethernet lmi interface**

Example:

```
Device(config-if)# ethernet lmi interface
```

Configures Ethernet LMI on the interface.

- When Ethernet LMI is enabled globally, it is enabled on all interfaces unless you disable it on specific interfaces. If Ethernet LMI is disabled globally, you can use this command to enable it on specified interfaces.

Step 5 **ethernet lmi** {**n393** *value* | **t392** *value*}

Example:

```
Device(config-if)# ethernet lmi n393 10
```

Configures Ethernet LMI parameters for the UNI.

Step 6 **end**

Example:

```
Device(config-if)# end
```

Returns to privileged EXEC mode.

Displaying Ethernet LMI and OAM Manager Information

Perform this task to display Ethernet Local Management Interface (LMI) or Operation, Administration, and Management (OAM) manager information. After step 1, all the steps are optional and can be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show ethernet lmi** {{**evc** [**detail** *evc-id* [**interface** *type number*] | **map interface** *type number*]} | {**parameters** | **statistics**} **interface** *type number* | **uni map** [**interface** *type number*]}
3. **show ethernet service evc** [**detail** | **id** *evc-id* [**detail**] | **interface** *type number* [**detail**]]
4. **show ethernet service instance** [**detail** | **id** *id* | **interface** *type number* | **policy-map** | **stats**]
5. **show ethernet service interface** [*type number*] [**detail**]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ethernet lmi** {{**evc** [**detail** *evc-id* [**interface** *type number*] | **map interface** *type number*]} | {**parameters** | **statistics**} **interface** *type number* | **uni map** [**interface** *type number*]}

Example:

```
Device# show ethernet lmi evc
```

Displays information that was sent to the customer edge (CE).

Step 3 **show ethernet service evc** [**detail** | **id** *evc-id* [**detail**] | **interface** *type number* [**detail**]]

Example:

```
Device# show ethernet service evc
```

Displays information about all Ethernet virtual circuits (EVCs) or about a specified EVC.

Step 4 **show ethernet service instance** [**detail** | **id** *id* | **interface** *type number* | **policy-map** | **stats**]

Example:

```
Device# show ethernet service instance detail
```

Displays information about customer service instances.

Step 5 **show ethernet service interface** [*type number*] [**detail**]

Example:

```
Device# show ethernet service interface ethernet 1/3 detail
```

Displays interface-only information about Ethernet customer service instances for all interfaces or for a specified interface.

Examples

The following example shows sample output from the **show ethernet lmi** command using the **evc** keyword:

```
Device# show ethernet lmi evc

St  EVC Id                                                  Port
--- ------------------------------------------------------ --------------
```

```
A  EVC_MP2MP_101                                                    Gi0/1
A  EVC_P2P_110                                                      Gi0/1
```

The following example is sample output from the **show ethernet service evc** command:

```
Device# show ethernet service evc

Identifier                    Type  Act-UNI-cnt Status
50                            MP-MP     0       NotDefined
```

The following is sample output from the **show ethernet service interface** command using the **detail** keyword:

```
Device#

Interface: Gigabitethernet
ID: uni2
CE-VLANS: 30
EVC Map Type: Bundling
Associated EVCs:
    EVC-ID                          CE-VLAN
    50                              30
Associated Service Instances:
    Service-Instance-ID CE-VLAN
    400                 30
```

The following is sample output from the **show ethernet service instance** command using the **detail** keyword:

```
Device# show ethernet service instance detail

Service Instance ID: 400
Associated Interface: GigabitEthernet
Associated EVC: 50
CE-Vlans: 30
State: AdminDown
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
```

Configuration Examples for Ethernet Local Management Interface at a Provider Edge

Example: Ethernet OAM Manager on a PE Device Configuration

This example shows a sample configuration of Operation, Administration, and Management (OAM) manager, Connectivity Fault Management (CFM), and Ethernet Local Management Interface (LMI) on a provider edge (PE) device. In this example, a bridge domain is specified.

```
Device> enable
Device# configure terminal
Device(config)# ethernet cfm global
Device(config)# ethernet cfm domain provider level 4
Device(config-ecfm)# service customer_1 evc test1 vlan 10
```

```
Device(config-ecfm-srv)# continuity-check
Device(config-ecfm-srv)# continuity-check interval 1s/10s/1m/10m
Device(config-ecfm-srv)# exit
Device(config-ecfm)# exit
Device(config)# ethernet evc test1
Device(config-evc)# uni count 3
Device(config-evc)# oam protocol cfm domain provider
Device(config-evc)# exit
Device(config)#
Device(config-if)# ethernet lmi interface
Device(config-if)# ethernet uni id CISCO
Device(config-if)# service instance 1 ethernet
Device(config-if-srv)# encapsulation untagged
Device(config-if-srv)# l2protocol peer
Device(config-if-srv)# bridge-domain 1
Device(config-if-srv)# exit
Device(config-if)# service instance 2 ethernet1
Device(config-if-srv)# ethernet lmi ce-vlan map 101
Device(config-if-srv)# encapsulation dot1q 2
Device(config-if-srv)# bridge-domain 2
Device(config-if-srv)# cfm mep domain provider mpid 10
Device(config-if-srv-ecfm-mep)# end
```

This example shows a configuration of OAM manager, CFM, and Ethernet LMI over an Xconnect configuration:

```
Device> enable
Device# configure terminal
Device(config)# ethernet cfm global
Device(config)# ethernet cfm domain provider level 4
Device(config-ecfm)# service customer_1 evc test1
Device(config-ecfm-srv)# continuity-check
Device(config-ecfm-srv)# continuity-check interval 1s,10s,1m,10m
Device(config-ecfm-srv)# exit
Device(config-ecfm)# exit
Device(config)# ethernet evc test1
Device(config-evc)# oam protocol cfm domain provider
Device(config-evc)# exit
Device(config)#
Device(config-if)# ethernet lmi interface
Device(config-if)# ethernet uni id CISCO
Device(config-if)# service instance 1 ethernet
Device(config-if-srv)# encapsulation untagged
Device(config-if-srv)# l2protocol peer
Device(config-if-srv)# bridge-domain 1
Device(config-if-srv)# exit
Device(config-if)# service instance 2 ethernet
Device(config-if-srv)# ethernet lmi ce-vlan map 101
Device(config-if-srv)# encapsulation dot1q 2
Device(config-if-srv)# xconnect 10.1.1.1 100 encapsulation mpls
Device(cfg-if-ether-vc-xconn)# exit
Device(config-if-srv)# cfm mep domain provider mpid 10
Device(config-if-srv-ecfm-mep)# end
```

Example: Ethernet LMI on a CE Device Configuration

This example shows how to configure Ethernet Local Management Interface (LMI) globally on a customer edge (CE) device:

```
Device# configure terminal
```

```
Device(config)# ethernet lmi global
Device(config)# ethernet lmi ce
Device(config)# exit
```

Additional References for Configuring Ethernet Local Management Interface at a Provider Edge

Related Documents

Related Topic	Document Title
Ethernet Connectivity Fault Management (CFM)	"Configuring Ethernet Connectivity Fault Management in a Service Provider Network" in the *Carrier Ethernet Configuration Guide*
Ethernet Local Management Interface (LMI)	"Enabling Ethernet Local Management Interface" in the *Carrier Ethernet Configuration Guide*
Remote Port Shutdown feature	"Configuring Remote Port Shutdown" in the *Carrier Ethernet Configuration Guide*
IEEE 802.3ah	*IEEE 802.3ah Ethernet in the First Mile*
Cisco high availability (HA) configuration information	*High Availability Configuration Guide*
Ethernet LMI commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Standards

Standard	Title
IEEE P802.1ag/D5.2	*Draft Standard for Local and Metropolitan Area Networks*
ITU-T	*ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks*
IETF VPLS OAM	*L2VPN OAM Requirements and Framework*
Metro Ethernet Forum 16 Technical Specification	*Technical Specification MEF 16- Ethernet Local Management Interface*
ITU-T Q.3/13	*Liaison statement on Ethernet OAM (Y.17ethoam)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Ethernet Local Management Interface at a Provider Edge

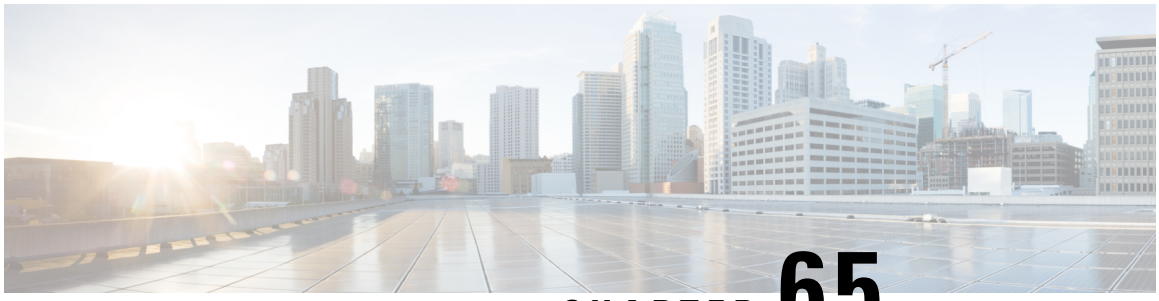
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 85: Feature Information for Configuring Ethernet Local Management Interface at a Provider Edge

Feature Name	Releases	Feature Information
Ethernet Local Management Interface at a Provider Edge	12.2(33)SRB 12.2(33)SXI	Ethernet LMI is an Ethernet OAM protocol between a CE device and a PE device. Ethernet LMI provides CE devices with the status of EVCs for large Ethernet MANs and WANs and provides information that enables CE devices to autoconfigure. Specifically, Ethernet LMI runs on the PE-CE UNI link and notifies a CE device of the operating state of an EVC and when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC. In Cisco IOS Release 12.2(33)SRB, this feature was introduced on the Cisco 7600 series router. The following commands were introduced or modified: **debug ethernet lmi**, **debug ethernet service, ethernet evc**, **ethernet lmi ce-vlan map**, **ethernet uni**, **oam protocol**, **service instance ethernet**, **show ethernet service evc**, **show ethernet service instance**, **show ethernet service interface, uni count**.

Feature Name	Releases	Feature Information
ISSU Support in E-LMI	12.2(33)SRD 15.0(1)S	ISSU allows you to perform a Cisco IOS software upgrade or downgrade without disrupting packet flow. ISSU lowers the impact that planned maintenance activities have on network availability by allowing software changes while the system is in service. In Cisco IOS Release 12.2(33)SRD, this feature was introduced on the Cisco 7600 series router. The following commands were introduced or modified: **debug ethernet lmi**.
NSF/SSO Support in E-LMI	12.2(33)SRD 15.0(1)S	The redundancy configurations SSO and NSF are supported in Ethernet LMI and are automatically enabled. A switchover from an active to a standby RP occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance. The primary function of Cisco NSF is to continue forwarding IP packets following an RP switchover. NSF also interoperates with the SSO feature to minimize network downtime following a switchover. In Cisco IOS Release 12.2(33)SRD, this feature was introduced on the Cisco 7600 series router. The following commands were introduced or modified: **debug ethernet lmi**.



CHAPTER 65

Using Link Layer Discovery Protocol in Multivendor Networks

Link Layer Discovery Protocol (LLDP), standardized by the IEEE as part of 802.1ab, enables standardized discovery of nodes, which in turn facilitates future applications of standard management tools such as Simple Network Management Protocol (SNMP) in multivendor networks. Using standard management tools makes physical topology information available and helps network administrators detect and correct network malfunctions and inconsistencies in configuration.

Media Endpoint Discovery (MED) is an LLDP enhancement that was formalized by the Telecommunications Industry Association (TIA) for voice over IP (VoIP) applications.

The Cisco implementation of LLDP is based on the IEEE 802.1ab standard. This document describes LLDP and LLDP-MED and how they are supported in Cisco software.

Prerequisites for Using Link Layer Discovery Protocol in Multivendor Networks

- Type-Length-Value (TLV) types 0 through 127
- To support LLDP-MED, the following organizationally specific TLVs must be implemented:
  - Extended Power-via-Media Dependent Interface (MDI)
  - Inventory
  - LLDP-MED Capabilities
  - MAC/PHY Configuration Status
  - Network Policy
  - Port VLAN ID

Restrictions for Using Link Layer Discovery Protocol in Multivendor Networks

- Use of LLDP is limited to 802.1 media types such as Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) networks.
- The maximum number of neighbor entries per chassis is limited on MED-capable network connectivity devices.

Information About Using Link Layer Discovery Protocol in Multivendor Networks

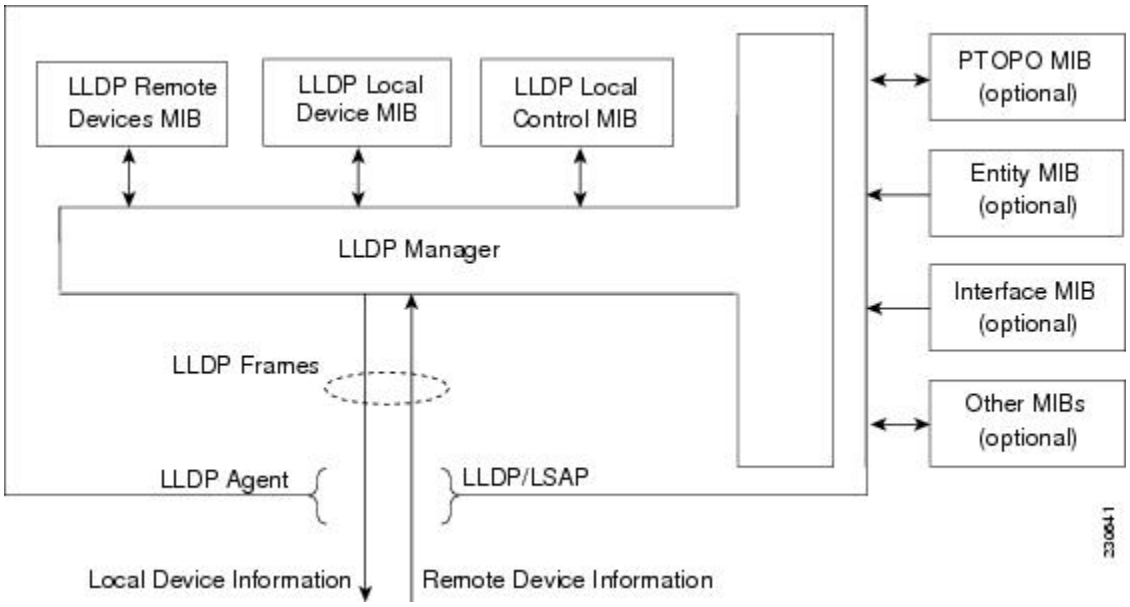
IEEE 802.1ab LLDP

IEEE 802.1ab Link Layer Discovery Protocol (LLDP) is an optional link layer protocol for network topology discovery in multivendor networks. Discovery information includes device identifiers, port identifiers, versions, and other details. As a protocol that aids network management, LLDP provides accurate network mapping, inventory data, and network troubleshooting information.

LLDP is unidirectional, operating only in an advertising mode. LLDP does not solicit information or monitor state changes between LLDP nodes. LLDP periodically sends advertisements to a constrained multicast address. Devices supporting LLDP can send information about themselves while they receive and record information about their neighbors. Additionally, devices can choose to turn off the send or receive functions independently. Advertisements are sent out and received on every active and enabled interface, allowing any device in a network to learn about all devices to which it is connected. Applications that use this information include network topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

Note LLDP and Cisco Discovery Protocol can operate on the same interface.

The figure below shows a high-level view of LLDP operating in a network node.



When you configure LLDP or Cisco Discovery Protocol location information on a per-port basis, remote devices can send Cisco medianet location information to the switch. For more information, see the *Using Cisco Discovery Protocol module.*

LLDP-MED

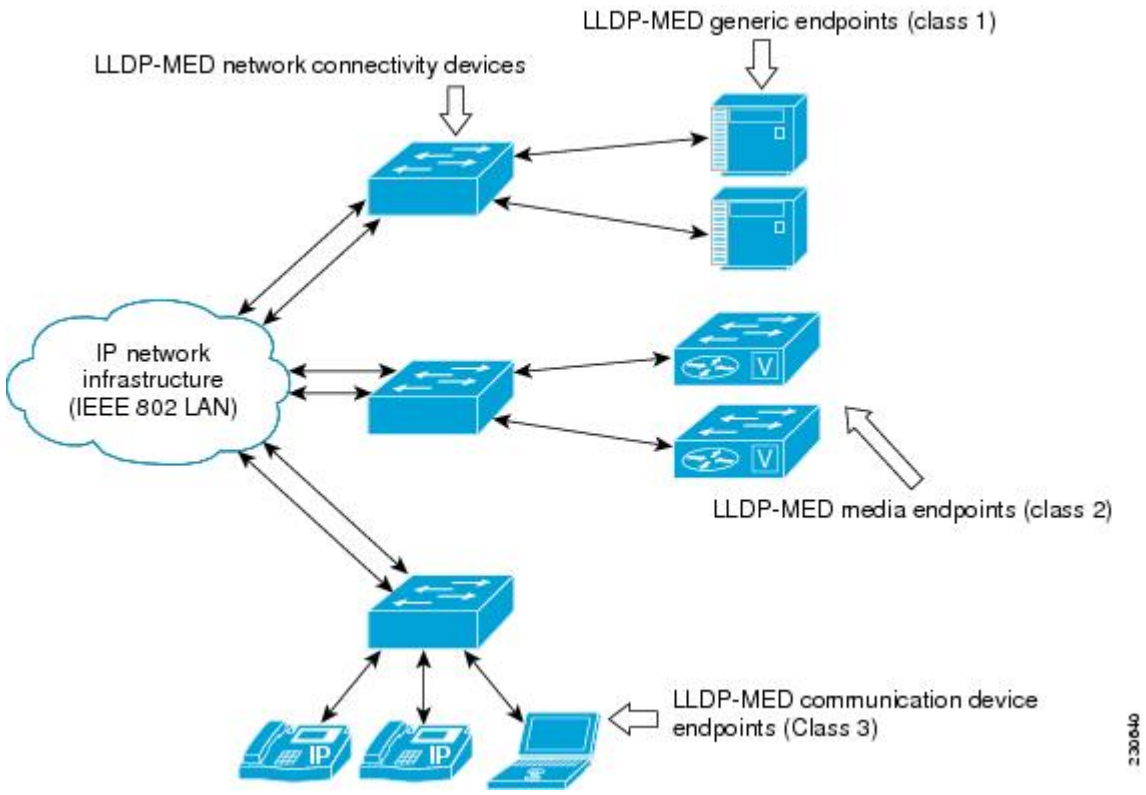
LLDP-MED operates between several classes of network equipment such as IP phones, conference bridges, and network connectivity devices such as routers and switches. By default, a network connectivity device sends out only LLDP packets until it receives LLDP-MED packets from an endpoint device. The network device then sends out LLDP-MED packets until the remote device to which it is connected ceases to be LLDP-MED capable.

Classes of Endpoints

LLDP-MED network connectivity devices provide IEEE 802 network access to LLDP-MED endpoints. LLDP-MED supports the following three classes of endpoints:

- Generic (class 1)—Basic participant endpoints; for example, IP communications controllers.
- Media (class 2)—Endpoints that support media streams; for example, media gateways and conference bridges.
- Communication Device (class 3)—Endpoints that support IP communications end users; for example, IP phones and Softphone.

The figure below shows an LLDP-MED-enabled LAN.



Types of Discovery Supported

LLDP-MED provides support to discover the following types of information, which are crucial to efficient operation and management of endpoint devices and the network devices supporting them:

- **Capabilities** —Endpoints determine the types of capabilities that a connected device supports and which ones are enabled.
- **Inventory** —LLDP-MED support exchange of hardware, software, and firmware versions, among other inventory details.
- **LAN speed and duplex** —Devices discover mismatches in speed and duplex settings.
- **Location identification** —An endpoint, particularly a telephone, learns its location from a network device. This location information may be used for location-based applications on the telephone and is important when emergency calls are placed.
- **Network policy** —Network connectivity devices notify telephones about the VLANs they should use.
- **Power** —Network connectivity devices and endpoints exchange power information. LLDP-MED provides information about how much power a device needs and how a device is powered. LLDP-MED also determines the priority of the device for receiving power.

Benefits of LLDP-MED

- Follows an open standard
- Supports E-911 emergency service, which is aided by location management

- Provides fast start capability
- Supports interoperability between multivendor devices
- Supports inventory management (location, version, etc.)
- Provides MIB support
- Supports plug and play installation
- Provides several troubleshooting (duplex, speed, network policy) mechanisms

TLV Elements

Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MED) use Type-Length-Values (TLVs) to exchange information between network and endpoint devices. TLV elements are embedded in communications protocol advertisements and used for encoding optional information. The size of the type and length fields is fixed at 2 bytes. The size of the value field is variable. The type is a numeric code that indicates the type of field that this part of the message represents, and the length is the size of the value field, in bytes. The value field contains the data for this part of the message.

LLDP-MED supports the following TLVs:

- LLDP-MED capabilities TLV—Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.
- Network policy TLV—Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any switch, obtain its VLAN number, and then start communicating with the call control.

By defining a network-policy profile TLV, you can create a profile for voice and voice signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. These profile attributes are then maintained centrally on the switch and propagated to the phone.

- Power management TLV—Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs. Supports advertisement of fractional wattage power requirements, endpoint power priority, and endpoint and network connectivity-device power status but does not provide for power negotiation between the endpoint and the network connectivity devices. When LLDP is enabled and power is applied to a port, the power TLV determines the actual power requirement of the endpoint device so that the system power budget can be adjusted accordingly. The switch processes the requests and either grants or denies power based on the current power budget. If the request is granted, the switch updates the power budget. If the request is denied, the switch turns off power to the port, generates a syslog message, and updates the power budget. If LLDP-MED is disabled or if the endpoint does not support the LLDP-MED power TLV, the initial allocation value is used throughout the duration of the connection.

Note A system power budget is the default power allocated to a device based on its device class. However, the total power that can be sourced from a switch is finite, and there will be some power budgeting done by the power module based on the number of ports already being served, total power that can be served, and how much new ports are requesting.

- Inventory management TLV—Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.
- Location TLV—Provides location information from the switch to the endpoint device. The location TLV can send this information:
  - Civic location information—Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.
  - ELIN location information—Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Benefits of LLDP

- Follows IEEE 802.1ab standard.
- Enables interoperability among multivendor devices.
- Facilitates troubleshooting of enterprise networks and uses standard network management tools.
- Provides extension for applications such as VoIP.

How to Configure Link Layer Discovery Protocol in Multivendor Networks

Enabling and Disabling LLDP Globally

LLDP is disabled globally by default. This section describes the tasks for enabling and disabling LLDP globally.

Enabling LLDP Globally

Perform this task to enable LLDP globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp run**
4. **end**

DETAILED STEPS

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 **lldp run**

Example:

```
Device(config)# lldp run
```

Enables LLDP globally.

Note To disable LLDP globally, use the **no lldp run** command.

Step 4 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Disabling and Enabling LLDP on a Supported Interface

LLDP is enabled by default on all supported interfaces. This section describes the tasks for disabling and enabling LLDP on a supported interface.

Disabling LLDP on a Supported Interface

Perform this task to disable LLDP on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no lldp** {**med-tlv-select** *tlv* | **receive** | **transmit**}
5. **end**

DETAILED STEPS

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** *type number*

Example:

```
Device(config)# interface Gigabitethernet 0/1
```

Specifies the interface type and number and enters interface configuration mode.

Step 4 **no lldp** {**med-tlv-select** *tlv* | **receive** | **transmit**}

Example:

```
Device(config-if)# no lldp receive
```

Disables an LLDP-MED TLV or LLDP packet reception on a supported interface.

Note To enable LLDP on a Supported Interface, use the **lldp** {**med-tlv-select** *tlv* | **receive** | **transmit** command.

Step 5 **end**

Example:

```
Device(config-if)# end
```

Returns to privileged EXEC mode.

Setting LLDP Packet Hold Time

Hold time is the duration that a receiving device should maintain LLDP neighbor information before aging it. Perform this task to define a hold time for an LLDP-enabled device.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **lldp holdtime** *seconds*
4. **end**

DETAILED STEPS

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 **lldp holdtime** *seconds*

Example:

```
Device(config)# lldp holdtime 100
```

Specifies the hold time.

Step 4 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Setting LLDP Packet Frequency

Perform this task to specify an interval at which the Cisco software sends LLDP updates to neighboring devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp timer** *rate*
4. **end**

DETAILED STEPS

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 **lldp timer** *rate*

Example:

```
Device(config)# lldp timer 75
```

Specifies the rate at which LLDP packets are sent every second.

Step 4 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Monitoring and Maintaining LLDP in Multivendor Networks

Perform this task to monitor and maintain LLDP in multivendor networks. This task is optional, and Steps 2 and 3 can be performed in any sequence.

SUMMARY STEPS

1. **enable**
2. **show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*]| **neighbors** [**ethernet** *number*| **detail**]| **traffic**]
3. **clear lldp** {**counters** | **table**}
4. **end**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*]| **neighbors** [**ethernet** *number*| **detail**]| **traffic**]

Example:

```
Device# show lldp entry *
```

Displays summarized and detailed LLDP information.

Note When the **show lldp neighbors** command is issued, if the device ID has more than 20 characters, the ID is truncated to 20 characters in command output because of display constraints.

Step 3 **clear lldp** {**counters** | **table**}

Example:

```
Device# clear lldp counters
```

Resets LLDP traffic counters and tables to zero.

Step 4 **end**

Example:

```
Device# end
```

Returns to user EXEC mode.

Enabling and Disabling LLDP TLVs

LLDP TLV support is enabled by default if LLDP is enabled globally and locally on a supported interface. Specific TLVs, however, can be enabled and suppressed.

Enabling LLDP TLVs

Perform this task to enable an LLDP TLV on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **lldp tlv-select** *tlv*
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** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/1`	Specifies the interface type and number on which to enable LLDP-MED and enters interface configuration mode.
Step 4	**lldp tlv-select** *tlv* **Example:** `Device(config-if)# lldp tlv-select power-management`	Enables a specific LLDP TLV on a supported interface. **Note** To disable LLDP TLVs, use the **no lldp tlv-select** *tlv*
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Enabling and Disabling LLDP-MED TLVs

LLDP-MED TLV support is enabled by default if LLDP is enabled globally and locally on a supported interface. Specific TLVs, however, can be enabled and suppressed.

Enabling LLDP-MED TLVs

Perform this task to enable a specific LLDP-MED TLV on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **lldp med-tlv-select** *tlv*
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** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/1`	Specifies the interface type and number on which to enable LLDP-MED and enters interface configuration mode.
Step 4	**lldp med-tlv-select** *tlv* **Example:** `Device(config-if)# lldp med-tlv-select inventory-management`	Enables a specific LLDP-MED TLV on a supported interface. **Note** To disable LLDP-MED TLVs, use the **no lldp med-tlv-select** *tlv* command.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Link Layer Discovery Protocol in Multivendor Networks

Example: Configuring Voice VLAN

The following example shows how to configure voice VLAN and verify

```
Device1> enable
Device1# configure terminal
Device1(config)# interface GigabitEthernet0/1/7
Device1(config-if)# switchport voice vlan 10
Device1(config-if)# no ip address
Device1(config-if)# end
```

The following example displays the updated running configuration on Device 2. LLDP is enabled with hold time, timer, and TLV options configured.

```
Device1# show lldp neighbors detail

Local Intf: Gi0/1/7
```

```
Chassis id: 10.10.0.1
Port id: C8F9F9D61BC2:P1
Port Description: SW PORT
System Name: SEPC8F9F9D61BC2

System Description:
Cisco IP Phone 7962G,V12, SCCP42.9-3-1ES27S

Time remaining: 127 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses:
    IP: 10.10.0.1
Auto Negotiation - supported, enabled
Physical media capabilities:
    1000baseT(HD)
    1000baseX(FD)
    Symm, Asym Pause(FD)
    Symm Pause(FD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

    MED Codes:
          (NP) Network Policy, (LI) Location Identification
          (PS) Power Source Entity, (PD) Power Device
          (IN) Inventory

    H/W revision: 12
    F/W revision: tnp62.8-3-1-21a.bin
    S/W revision: SCCP42.9-3-1ES27S
    Serial number: FCH1610A5S5
    Manufacturer: Cisco Systems, Inc.
    Model: CP-7962G
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN 10, tagged, Layer-2 priority: 5, DSCP: 46
    Network Policy(Voice Signal): VLAN 10, tagged, Layer-2 priority: 4, DSCP: 32
    PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 6.3
    Location - not advertised
```

The following example shows how to configure LLDP timer, hold time, and TLVs options on Device 2.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# lldp run
Device(config)# lldp holdtime 150
Device(config)# lldp timer 15
Device(config)# lldp tlv-select port-vlan
Device(config)# lldp tlv-select mac-phy-cfg
Device2(config)# interface ethernet 0/0
Device2(config-if)# lldp transmit
Device2(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows that voice vlan has been configured on the IP phone.

```
Device1# show lldp traffic
LLDP traffic statistics:
    Total frames out: 20
    Total entries aged: 0
    Total frames in: 15
```

```
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
Device1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device2             Et0/0          150        R               Et0/0
Total entries displayed: 1
Device2# show lldp traffic
LLDP traffic statistics:
    Total frames out: 15
    Total entries aged: 0
    Total frames in: 17
    Total frames received in error: 0
    Total frames discarded: 2
    Total TLVs unrecognized: 0
Device2# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device1             Et0/0          150        R               Et0/0
Total entries displayed: 1
```

Example Configuring LLDP on Two Devices

The following example shows how to configure LLDP timer, hold time, and TLVs on two devices in a network. In each case we assume that the Ethernet interfaces being configured are in the UP state.

```
! Configure LLDP on Device 1 with hold time, timer, and TLV options.

Device1> enable
Device1# configure terminal
Device1(config)# lldp run
Device1(config)# lldp holdtime 150
Device1(config)# lldp timer 15
Device1(config)# lldp tlv-select port-vlan
Device1(config)# lldp tlv-select mac-phy-cfg
Device1(config)# interface ethernet 0/0
Device1(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console
! Show the updated running configuration. LLDP is enabled with hold time, timer, and TLV
options configured.

Device1# show running-config

Building configuration...
Current configuration : 1397 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Device1
!
boot-start-marker
boot-end-marker
!
```

```
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
!
!
lldp timer 15
lldp holdtime 150
!


! Configure LLDP on Device 2 with hold time, timer, and TLV options.

Device2> enable
Device2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device2(config)# lldp run
Device2(config)# lldp holdtime 150
Device2(config)# lldp timer 15
Device2(config)# lldp tlv-select port-vlan
Device2(config)# lldp tlv-select mac-phy-cfg
Device2(config)# interface ethernet 0/0
Device2(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console

! Show the updated running configuration on Device 2. LLDP is enabled with hold time, timer,
 and TLV options configured.

Device2# show running-config
Building configuration...
Current configuration : 1412 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
!
!
lldp timer 15
lldp holdtime 150
!


! After both devices are configured for LLDP, issue the show
 command from each device to view traffic and device information.

Device1# show lldp traffic
LLDP traffic statistics:
    Total frames out: 20
    Total entries aged: 0
    Total frames in: 15
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
```

```
Device1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device2             Et0/0          150        R               Et0/0
Total entries displayed: 1
Device2# show lldp traffic
LLDP traffic statistics:
    Total frames out: 15
    Total entries aged: 0
    Total frames in: 17
    Total frames received in error: 0
    Total frames discarded: 2
    Total TLVs unrecognized: 0
Device2# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device1             Et0/0          150        R               Et0/0
Total entries displayed: 1
```

Feature Information for Link Layer Discovery Protocol in Multivendor Networks

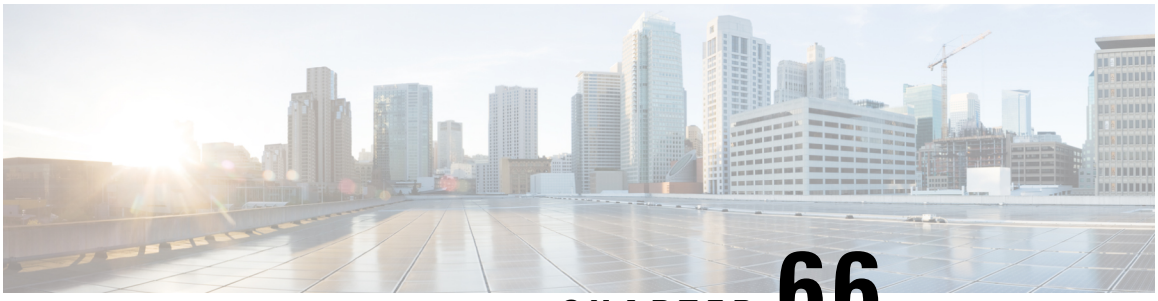
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 86: Feature Information for Using Link Layer Discovery Protocol in Multivendor Networks

Feature Name	Releases	Feature Information
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)		LLDP, standardized by the IEEE as part of 802.1ab, enables standardized discovery of nodes, which in turn facilitates future applications of standard management tools such as SNMP in multivendor networks. The following commands were introduced or modified: **clear lldp**, **lldp** and **show lldp**.
ANSI TIA-1057 LLDP-MED Support		MED is an LLDP enhancement that was formalized by the TIA for VoIP applications. The Cisco implementation of LLDP is based on the IEEE 802.1ab standard. The following commands were introduced or modified: **lldp** and **lldp** (interface).

Feature Name	Releases	Feature Information
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Cisco IOS XE Release 3.2E Cisco IOS XE Release 3.6E	IEEE 802.3ad link bundling and load balancing leverages the EtherChannel infrastructure within Cisco software to manage the bundling of various links. The network traffic load-balancing features help minimize network disruption that results when a port is added or deleted from a link bundle. MED is an LLDP enhancement that was formalized by the TIA for VoIP applications. In Cisco IOS XE Release 3.2SE, this feature is supported on the following platforms: • Cisco 5700 Series Wireless LAN Controllers • Cisco Catalyst 3850 Series Switches In Cisco IOS XE Release 3.3SE, this feature is supported on the following platforms: • Cisco Catalyst 3650 Series Switches
LLDP MED Support on ISRG2		The LLDP MED feature is supported on Cisco Integrated Services Routers Generation 2 (ISR G2). No commands were introduced or modified.



CHAPTER 66

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

- 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 **lacp min-bundle** 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 active 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

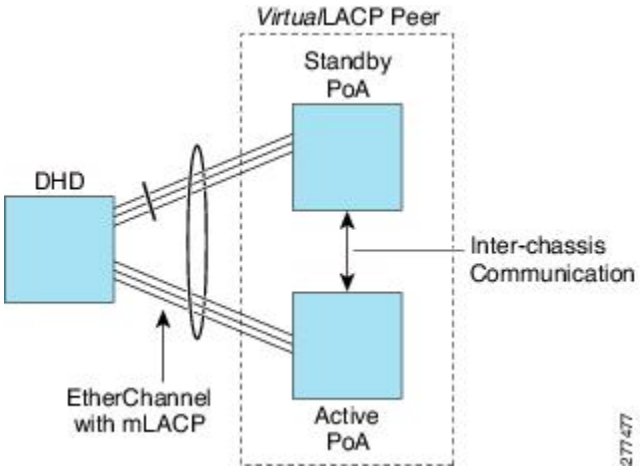
- mLACP does not support Fast Ethernet.
- mLACP does not support half-duplex links.
- mLACP does not support multiple neighbors.
- Converting a port channel to mLACP can cause a service disruption.
- The maximum number of member links per LAG per PoA is restricted by the maximum number of ports per port 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.

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

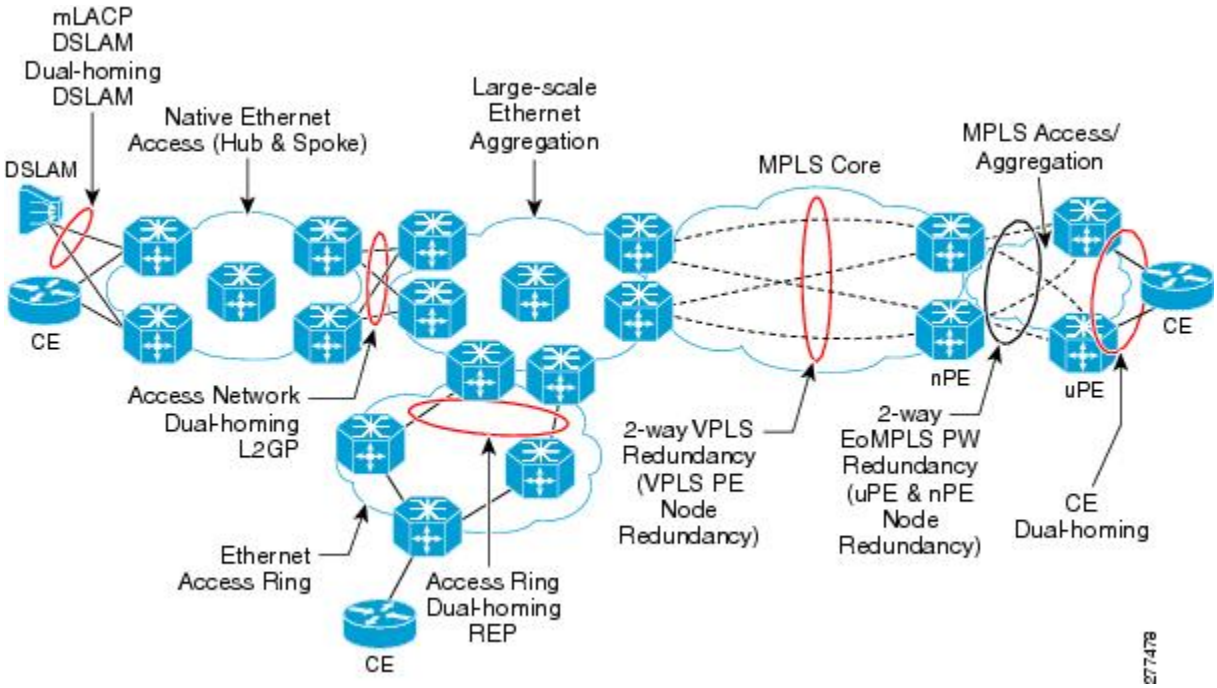
The Carrier Ethernet redundancy solution should include the following processes (and how they apply to the mLACP solution):

- 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 failure. 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 Failure occurs when incoming traffic is dropped without informing the source that the data did not reach its intended recipient. Failure 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.



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.

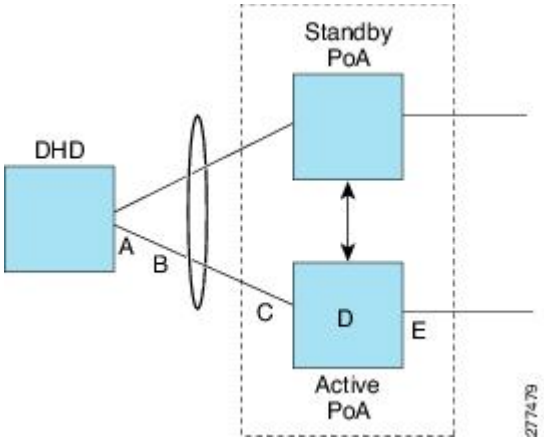
Port Key

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 example, 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 value of PoAs must be greater than the value of DHD. In DHD-based control, maximum number of links per bundle should be one. The PoAs must be configured to limit the maximum number of links per bundle to be 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. 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 **lacp 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 interchassis** command follows:

```
Device# show redundancy interchassis
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 87: 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.
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 failure.

At the failover from a primary PoA to a secondary PoA, a service experiences traffic failure 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 failure continues until the remote devices age out their stale MAC address table entries (which typically takes five minutes). To prevent this

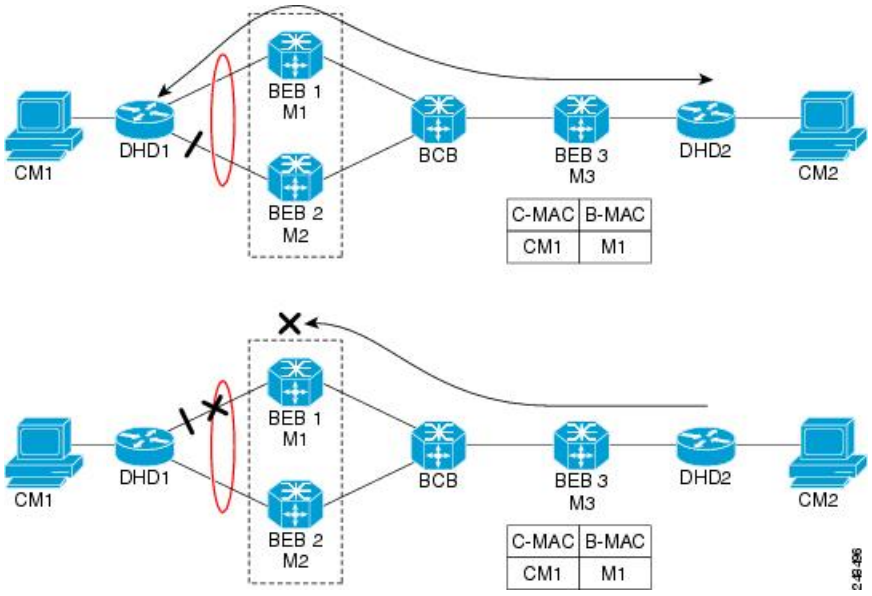
anomaly, the newly active PoA, which has taken control of the service, transmits a MAC flush notification message to the remote devices in the network to flush their stale MAC address entries for the service in question.

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.



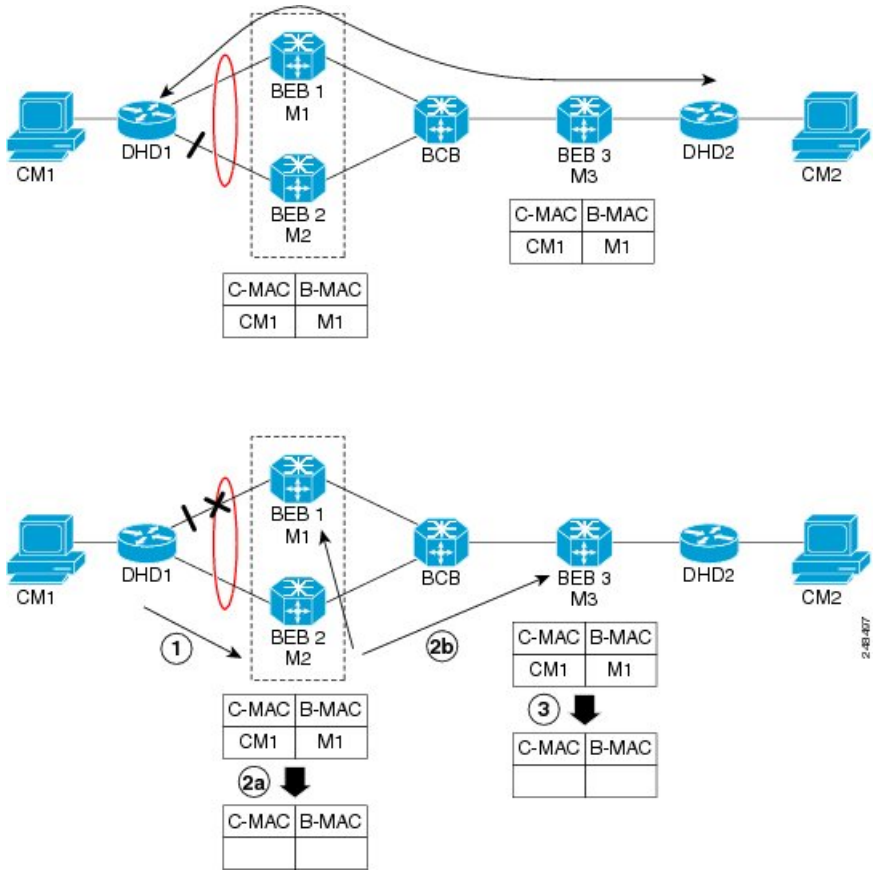
Device DHD1 is dual-homed to two 802.1ah backbone edge bridges (BEB1 and BEB2). Assume that initially the primary path is through BEB1. In this configuration BEB3 learns that the host behind DHD1 (with MAC address CM1) is reachable via the destination B-MAC M1. If the link between DHD1 and BEB1 fails 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 fails.

To circumvent the traffic failure 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 (Global Redundancy Group Configuration)

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

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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.

Step 4 **interchassis group** *group-id*

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** *ip-address*

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.

- 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.

- The format of the *mac-address* argument must be in standard MAC address format: aabb.ccdd.eeff.

Step 9 **mlacp system-priority** *priority-value*

Example:

```
Router(config-r-ic)# mlacp system-priority 100
```

Defines the system priority advertised to the other mLACP members of the redundancy group.

- System priority values are 1 to 65535. Default value is 32768.
- The assigned values should be lower than the DHD.

Step 10 **backbone interface** *type number*

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 (Global Redundancy Group Configuration) , on page 899.

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. **exit**
10. **exit**
11. **errdisable recovery cause mlacp-minlink**
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 4	**lacp max-bundle** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 4`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles* argument should not be less than the total number of links in the LAG that are connected to the PoA. • 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 5	**lacp failover** {**brute-force**| **non-revertive**} **Example:** `Router(config-if)# lacp failover brute-force`	Sets the mLACP switchover to nonrevertive or brute force. This command is optional. • 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:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 8	**interchassis group** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port channel. The *group-id* should match the configured redundancy group.
Step 9	**exit** **Example:** `Router(config-r-ic)# exit`	Exits interchassis redundancy mode.
Step 10	**exit** **Example:** `Router(config-red)# exit`	Exits redundancy configuration mode.
Step 11	**errdisable recovery cause mlacp-minlink** **Example:** `Router(config)# errdisable recovery cause mlacp-minlink`	Enables automatic recovery from a failover state of the port channel.
Step 12	**end** **Example:** `Router(config)# end`	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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *pw-class-name* **Example:** `Router(config)# pseudowire-class ether-pw`	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.

	Command or Action	Purpose
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** *port-channel-number* **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** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 4`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • Determines whether the redundancy group is under DHD control, PoA control, or both. • Range is 1 to 8. Default value is 8.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 12	**redundancy** **Example:**	Enters redundancy configuration mode.

	Command or Action	Purpose
	`Router(config)# redundancy`	
Step 13	**interchassis group** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port channel. • The *group-id* 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** *port-channel-number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 17	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance.
Step 18	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**native**] **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 19	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode.
Step 20	**xconnect** *peer-ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] **Example:** `Router(config-if)# xconnect 10.0.3.201 123 pw-class ether-pw`	Binds an attachment circuit to a pseudowire.
Step 21	**backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*]	Specifies a redundant peer for a pseudowire virtual circuit.

	Command or Action	Purpose
	Example: `Router(config-if)# backup peer 10.1.1.1 123 pw-class ether-pw`	
Step 22	**end** **Example:** `Router(config-if)# end`	Returns the CLI to privileged EXEC mode.

Configuring Redundancy for VPWS on ME3600 Series Switches

Perform this task to provide Layer 2 VPN service redundancy for VPWS on Cisco ME3600, ME3600X 24CX, ME3800 series switches.

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. **switchport mode trunk**
9. **switchport trunk allowed vlan none**
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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *pw-class-name* **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** *port-channel-number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 8	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Specifies the port channel as trunking VLAN Layer 2 interface.
Step 9	**switchport trunk allowed vlan none** **Example:** `Router(config-if)# switchport trunk allowed vlan none`	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.

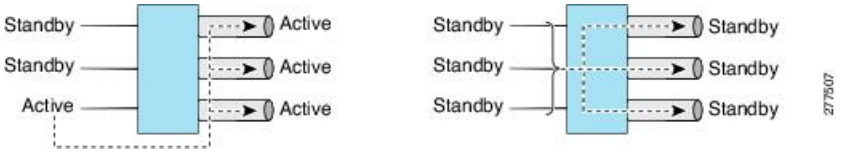
	Command or Action	Purpose
Step 10	**lacp fast-switchover** **Example:** `Router(config-if)# lacp fast-switchover`	Enables LACP 1-to-1 link redundancy.
Step 11	**lacp max-bundle** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 4`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • 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** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port channel. • The *group-id* 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.
Step 17	**interface port-channel** *port-channel-number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 18	**service instance** *id* **ethernet** [*evc-name*] **Example:**	Configures an Ethernet service instance.

	Command or Action	Purpose
	`Router(config-if)# service instance 1 ethernet`	
Step 19	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**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** *peer-ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}] **Example:** `Router(config-if)# xconnect 10.0.3.201 123 pw-class ether-pw`	Binds an attachment circuit to a pseudowire.
Step 22	**backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*] **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.

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. However, if the attachment circuit is down, all pseudowires also go down. 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**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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. • 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.
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:**	Enables LACP 1-to-1 link redundancy.

	Command or Action	Purpose
	`Router(config-if)# lacp fast-switchover`	
Step 11	**lacp max-bundle** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 2`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • 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** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port-channel. • The *group-id* 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.
Step 17	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 18	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance and enters Ethernet service configuration mode.

	Command or Action	Purpose
Step 19	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**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** *bridge-id* [**split-horizon** [**group** *group-id*]] **Example:** `Router(config-if-srv)# bridge-domain 200`	Configures the bridge domain. Binds the service instance to a bridge domain instance where *domain-number* 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** *vlanid* **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** *vfi-name* **Example:** `Router(config-if)# xconnect vfi vfi-16`	Specifies the Layer 2 VFI that you are binding to the VLAN port.
Step 25	**end** **Example:** `Router(config-if)# end`	Returns the CLI to privileged EXEC mode.

Steps for Configuring Redundancy for VPLS on ME3600 Series Switches

Perform the following task to configure redundancy for VPLS on Cisco ME3600, ME3600X 24CX, ME3800 series switches.

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. **switchport mode trunk**
10. **switchport trunk allowed vlan none**
11. **lacp fast-switchover**
12. **lacp max-bundle** *max-bundles*
13. **exit**
14. **redundancy**
15. **interchassis group** *group-id*
16. **exit**
17. **exit**
18. **interface port-channel** *port-channel- number*
19. **service instance** *id* **ethernet** [*evc-name*]
20. **encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**native**]
21. **bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]]
22. **exit**
23. **interface vlan** *vlanid*
24. **no ip address**
25. **xconnect vfi** *vfi-name*
26. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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.

	Command or Action	Purpose
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. • 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.
Step 9	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Specifies the port channel as trunking VLAN Layer 2 interface.
Step 10	**switchport trunk allowed vlan none** **Example:** `Router(config-if)# switchport trunk allowed vlan none`	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
Step 11	**lacp fast-switchover** **Example:** `Router(config-if)# lacp fast-switchover`	Enables LACP 1-to-1 link redundancy.
Step 12	**lacp max-bundle** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 2`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • 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 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 14	**redundancy** **Example:** `Router(config)# redundancy`	• Enters redundancy configuration mode.
Step 15	**interchassis group** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port-channel. • The *group-id* should match the configured redundancy group.
Step 16	**exit** **Example:** `Router(config-r-ic)# exit`	Exits interchassis redundancy mode.
Step 17	**exit** **Example:** `Router(config-red)# exit`	Exits redundancy configuration mode.
Step 18	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 19	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance and enters Ethernet service configuration mode.
Step 20	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**native**] **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
Step 21	**bridge-domain** *bridge-id* [**split-horizon** [**group** *group-id*]] **Example:** `Router(config-if-srv)# bridge-domain 200`	Configures the bridge domain. Binds the service instance to a bridge domain instance where *domain-number* is the identifier for the bridge domain instance.

	Command or Action	Purpose
Step 22	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode.
Step 23	**interface vlan** *vlanid* **Example:** `Router(config-if)# interface vlan 200`	Creates a dynamic switch virtual interface (SVI).
Step 24	**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 25	**xconnect vfi** *vfi-name* **Example:** `Router(config-if)# xconnect vfi vfi-16`	Specifies the Layer 2 VFI that you are binding to the VLAN port.
Step 26	**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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *pw-class-name* **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:**	Exits pseudowire class configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Router(config-pw-class)# exit`	
Step 8	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
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** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 4`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • 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** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port channel. • The *group-id* should match the configured redundancy group.
Step 15	**exit** **Example:** `Router(config-r-ic)# exit`	Exits interchassis redundancy mode.

	Command or Action	Purpose
Step 16	**exit** **Example:** `Router(config-red)# exit`	Exits redundancy configuration mode.
Step 17	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 18	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance and enters Ethernet service configuration mode.
Step 19	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**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** *peer-ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**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** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*] **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.

Configuring Hierarchical VPLS on ME3600 Series Switches

Perform this task to configure Hierarchical VPLS (H-VPLS) on Cisco ME3600, ME3600X 24CX, ME3800 series switches.

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. **switchport mode trunk**
10. **switchport trunk allowed vlan none**
11. **lacp fast-switchover**
12. **lacp max-bundle** *max-bundles*
13. **exit**
14. **redundancy**
15. **interchassis group** *group-id*
16. **exit**
17. **exit**
18. **interface port-channel** *port-channel- number*
19. **service instance** *id* **ethernet** [*evc-name*]
20. **encapsulation dot1q** *vlan-id* [**,** *vlan-id*[**-** *vlan-id*]] [**native**]
21. **exit**
22. **xconnect** *peer-ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]
23. **backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*]
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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** *pw-class-name* **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** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 9	**switchport mode trunk** **Example:** `Router(config-if)# switchport mode trunk`	Specifies the port channel as trunking VLAN Layer 2 interface.
Step 10	**switchport trunk allowed vlan none** **Example:** `Router(config-if)# switchport trunk allowed vlan none`	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode.
Step 11	**lacp fast-switchover** **Example:** `Router(config-if)# lacp fast-switchover`	Enables LACP 1-to-1 link redundancy.

	Command or Action	Purpose
Step 12	**lacp max-bundle** *max-bundles* **Example:** `Router(config-if)# lacp max-bundle 4`	Configures the max-bundle links that are connected to the PoA. The value of the *max-bundles*argument should not be less than the total number of links in the LAG that are connected to the PoA. • Determines whether the redundancy group is under DHD control, PoA control, or both. • Range is 1 to 8. Default value is 8.
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 14	**redundancy** **Example:** `Router(config)# redundancy`	Enters redundancy configuration mode.
Step 15	**interchassis group** *group-id* **Example:** `Router(config-red)# interchassis group 230`	Specifies that the port channel is an mLACP port channel. • The *group-id* should match the configured redundancy group.
Step 16	**exit** **Example:** `Router(config-r-ic)# exit`	Exits interchassis redundancy mode.
Step 17	**exit** **Example:** `Router(config-red)# exit`	Exits redundancy configuration mode.
Step 18	**interface port-channel** *port-channel- number* **Example:** `Router(config)# interface port-channel1`	Configures the port channel and enters interface configuration mode.
Step 19	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet`	Configures an Ethernet service instance and enters Ethernet service configuration mode.
Step 20	**encapsulation dot1q** *vlan-id* [**,** *vlan-id*[- *vlan-id*]] [**native**] **Example:**	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.

	Command or Action	Purpose
	`Router(config-if-srv)# encapsulation dot1q 100`	
Step 21	**exit** **Example:** `Router(config-if-srv)# exit`	Exits service instance configuration mode.
Step 22	**xconnect** *peer-ip-address vc-id* {**encapsulation mpls** | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**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 23	**backup peer** *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*] **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 24	**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.

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **debug redundancy interchassis** {**all** | **application** | **error** | **event** | **monitor**}

Example:

```
Router# debug redundancy interchassis all
```

- Enables debugging of the interchassis redundancy manager.

Step 3 **debug mpls ldp iccp**

Example:

```
Router# debug mpls ldp iccp
```

- 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.

- This command is run on the switch processor.

Step 5 **debug lacp etherchannel**

Example:

```
Router# debug lacp etherchannel
```

Enables debugging for etherchannel component.

Debugging mLACP on an Attachment Circuit or EVC

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

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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.

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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.

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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.

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.

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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).

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- 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.

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

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
```

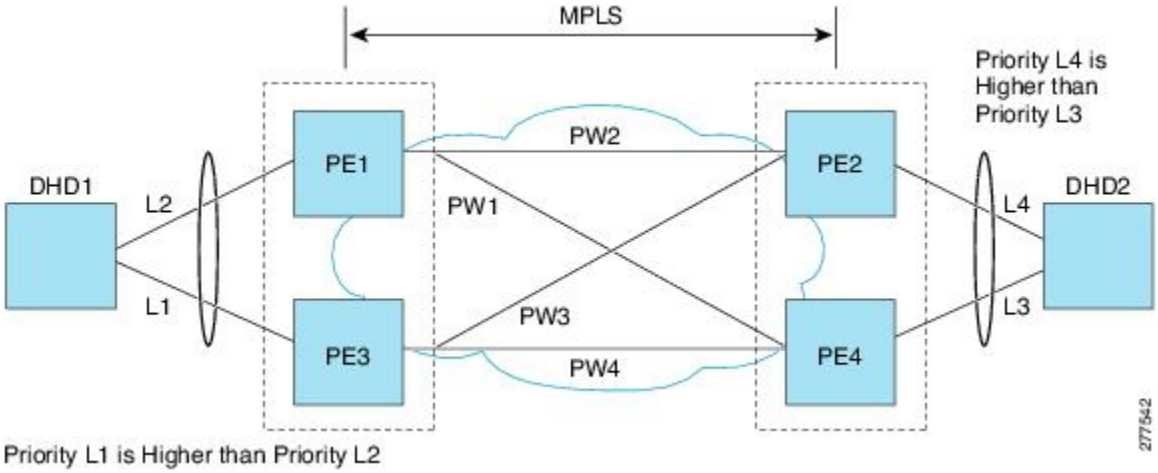
Enables the display of VFI events when AToM is configured for NSF/SSO and Graceful Restart.

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

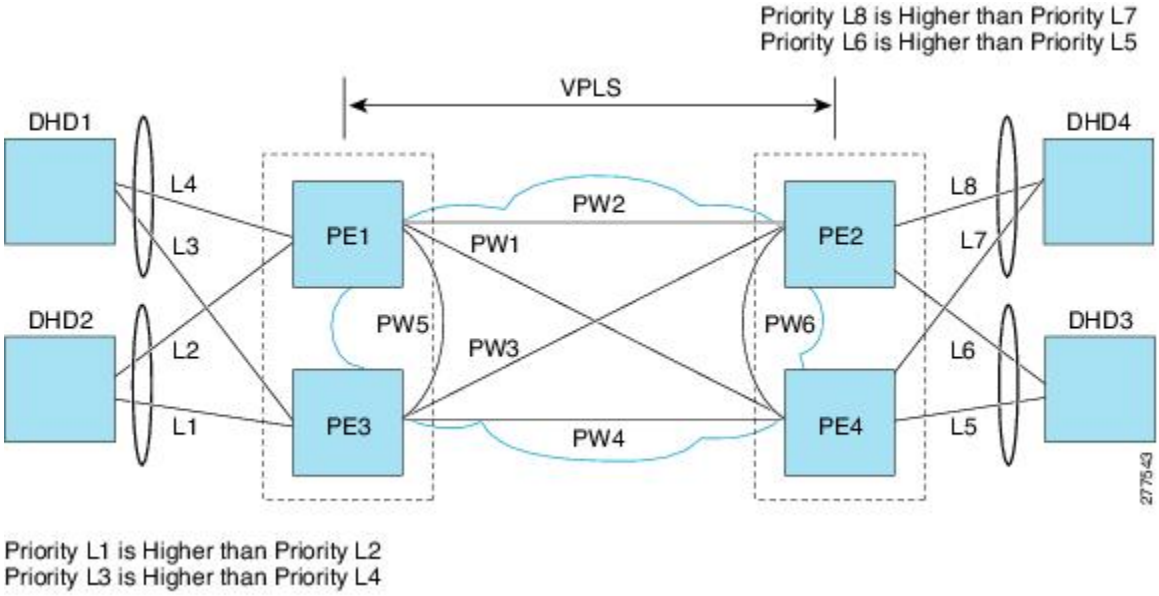
The following VPWS sample configuration is for a standby PoA:

```
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

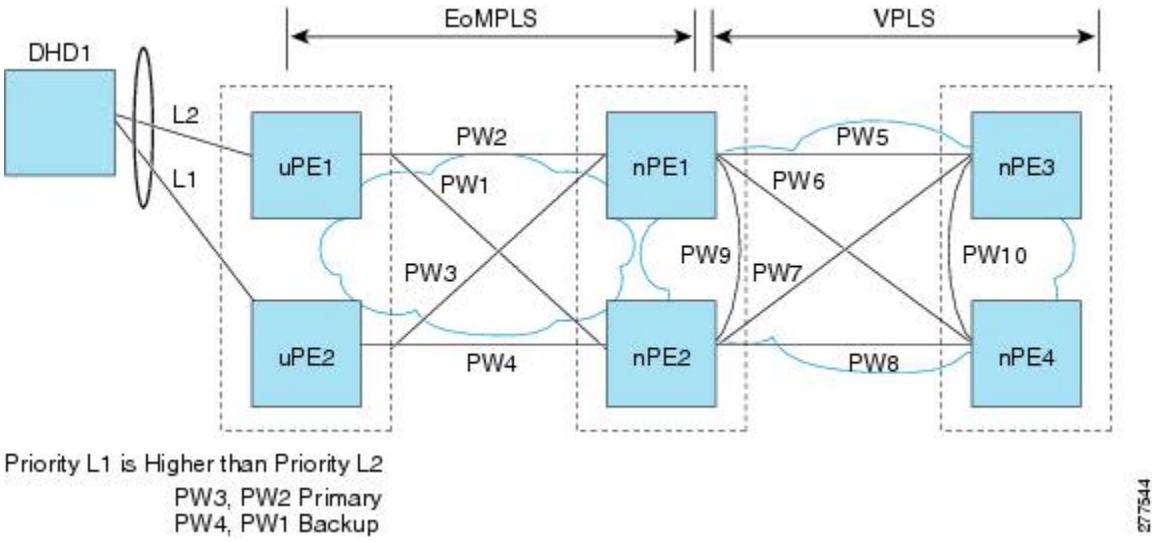
The following VPLS sample configuration is for a standby PoA:

```
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 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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
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
-------------  -------------------------- --------------- ---------- ----------
Po1            Eth VLAN 2                 172.2.2.2       2          STANDBY
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      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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
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
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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
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

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

showetherchannelsummary

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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
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
```

Feature Information for mLACP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 88: Feature Information for mLACP

Feature Name	Releases	Feature Information
Multichassis LACP (mLACP)		Cisco's mLACP feature addresses the need for interchassis redundancy mechanisms when a carrier wants to dual home a device to two upstream PoAs for redundancy. The mLACP feature enhances the 802.3ad LACP implementation to meet this requirement. The following commands were introduced or modified: **backbone interface**, **debug acircuit checkpoint**, **debug lacp**, **ethernet mac-flush mirp notification**, **interchassis group**, **lacp failover**, **lacp max-bundle**, **lacp min-bundle**, **member ip**, **mlacp interchassis group**, **mlacp lag-priority**, **mlacp node-id**, **mlacp system-mac**, **mlacp system-priority**, **monitor peer bfd**, **redundancy**, **show ethernet service instance interface port-channel**, **show ethernet service instance id mac-tunnel**, **show lacp**, **status decoupled**, **status peer topology dual-homed**.

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.

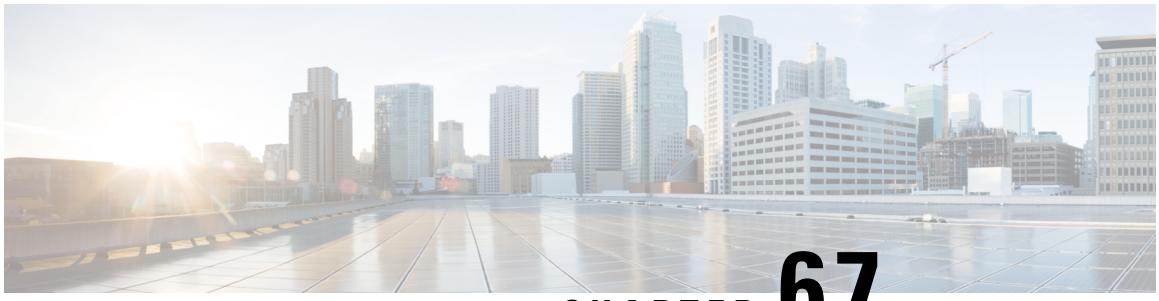
standby attachment circuit—The link that is in standby mode between the DHD and the standby PoA.

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.



CHAPTER 67

ICCP Multichassis VLAN Redundancy

Carrier Ethernet network high availability can be achieved by employing intra- and inter-chassis redundancy mechanisms. The Multichassis Link Aggregation Control Protocol (mLACP) solution addresses the latter, where a carrier wants dual-homed device (DHD) to two upstream points of attachment (PoA) for redundancy. Some carriers do not run loop prevention control protocols in their access networks, so an alternate redundancy scheme is necessary.

The implementation of mLACP supports DHD with an active/standby topology. Interchassis Communication Protocol (ICCP) Multichassis VLAN Redundancy, also known as Pseudo mLACP, provides a flexible dual-homing redundancy mechanism. It uses similar principles as mLACP. The Pseudo mLACP solution extends the mLACP functionality to support active/active PoAs deployments. This enables flexibility in network planning and efficient resource utilization.

Pseudo mLACP has the following advantages over mLACP:

- Pseudo mLACP supports per-VLAN active/active redundancy without any load-balancing requirements on the CE.
- Pseudo mLACP is independent of the access redundancy mechanism; therefore, it provides a network-based redundancy solution. It allows maximum flexibility for the Provider Edge (PE)-Customer Edge (CE) interoperability in terms of dual-homing redundancy and recovery.

Prerequisites for ICCP Multichassis VLAN Redundancy

- mLACP support is required for Pseudo mLACP.

Restrictions for ICCP Multichassis VLAN Redundancy

- Max bundle should not be configured on a Pseudo mLACP enabled port channel.
- Pseudo mLACP does not work with most of the Layer 2 control protocols or Spanning Tree Protocol (STP) including Multiple Spanning Tree Protocol (MSTP) or VLAN Trunking Protocol (VTP).
- When a service instance is configured under a Pseudo mLACP port channel, all the outer tag VLANs of a service instance must be a part of either a primary VLAN list or a secondary VLAN list.
- Outer VLANs of one service instance cannot be mixed with the primary and secondary VLAN list on a Pseudo mLACP port channel.
- Brute-Force mode configuration is not supported.
- VLAN force-switchover configuration is applicable only for nonrevertive mode.
- The DHD nodes must support the LACP functionality.
- The DHD nodes must support MVRP MAC flush functionality in Pseudo mLACP topology.

Information About ICCP Multichassis VLAN Redundancy

Pseudo mLACP Multihoming Redundancy

The provider edge (PE) ports are configured in such a way that they act as if connected to a virtual device over a Multichassis link aggregation group (MC-LAG) with mLACP. Points of Attachment (PoAs) can be placed in active/active mode with manual VLAN load balancing. DHD ports are configured into two individual port channels that are physically connected to each of the PoAs. Interchassis Communication Protocol (ICCP), with new extensions is used for interchassis communication to control the failover process. Multiple VLAN Registration Protocol (MVRP) lite is used for active VLAN notification and MAC flushing toward the access side. For MAC flushing notification toward the core, MVRP lite, Multiple I-SID Registration Protocol (MIRP) lite, or LDP MAC withdraw can be used.

Pseudo mLACP provides:

- The active/active mode redundancy of two PoAs in a redundancy group. This provides higher bandwidth utilization than mLACP and other active/standby link-level schemes. Pseudo mLACP eliminates the required wasted link bandwidth on the standby PoA.
- Flexible access network topologies, that is, access network dual-homing and access device dual-homing.
- Service provider control over the provisioning, role assignment, failover, and load sharing between PoAs.
- PE node redundancy for Virtual Private Wire Service (VPWS), Virtual Private LAN Service (VPLS), and native Ethernet aggregation.

The DHD is configured with two different port channels that are connected to a single multichassis LAG (mLAG) on the PoA side. The LACP module on the PoAs receives two different port keys from the two different port channels on the DHD. The mLAG on the PoA ignores the port keys from the DHD's LACP PDUs to form a single bundle on the PoA side.

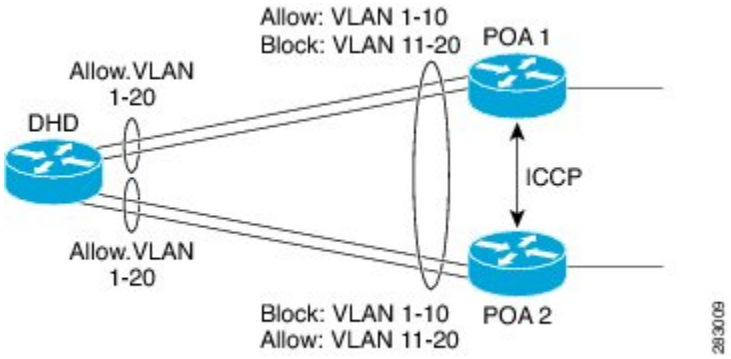
The mLACP module provides failover and recovery notifications to Pseudo mLACP. Reversion delay is processed by the mLACP module. mLACP provides a CLI interface for Pseudo mLACP VLANs and mode configuration. mLACP supports VLAN-based active/active redundancy, in addition to PoA-level active/standby redundancy. VLAN-based active/active redundancy allows you to bundle links on both the PoAs based on the Pseudo mLACP configuration. Pseudo mLACP and mLACP port-channels can be configured together on the same pair of PoAs, and both can use the same redundancy group.

After failover, the new active PoA activates the standby VLAN list on the port-channel. However, to receive traffic on the newly active VLAN's DHD, networks must flush their MAC address table and learn the new MAC address of the new PoA port channel interface. The existing MVRP lite support is used for DHD-side MAC flushing.

Pseudo mLACP Active/Active Support

Pseudo mLACP supports active/active redundancy without the restriction of symmetric VLAN-based load sharing in both the Provider Edge (PE) and the Customer Edge (CE).

Figure 39: Active/Active Support



Pseudo mLACP provides VLAN-based redundancy by allowing you to specify one primary interface and one secondary interface or a PoA pair for each member VLAN. The configuration determines the PoA that will be initially active for a VLAN, by using the primary and secondary VLAN lists under the Pseudo mLACP interface. Only the active PoA will forward frames for the respective VLANs. The standby PoA will be in the blocking mode (bidirectional), dropping all the frames received on the standby VLANs. The failover will occur for all the VLANs in the active/standby list and not on a per-VLAN basis. Pseudo mLACP provides per-port-channel VLAN load balancing. You can statistically configure the primary and secondary VLAN list on each of the PoAs.

The DHD nodes are configured such that each of their uplinks to a PoA operates as an individual port channel. Each interface must be configured to forward all local VLANs on all uplinks belonging to the mLAG.

The data-path forwarding scheme causes the DHD to automatically learn which PoA or interface is active for a given VLAN. This learning occurs at an individual destination MAC address level.

Failure Recovery

Pseudo mLACP uses revertive behavior (which is the default behavior) after the failure recovery to support the active/active model. You can configure a nonrevertive mode.

Reversion occurs the same way that the original failover occurs. The reversion must be initiated by the new active PoA for the given VLANs, by signaling that the PoA is relinquishing its active role for the VLAN. This is done through an ICCP Pseudo mLACP port-state TLV, which indicates that it is no longer in the active mode for the affected VLANs. Upon a TLV receipt, the recovering PoA unblocks the affected VLANs, and triggers MAC flushes toward both the access side and the core side).

mLACP reversion delay applies for Pseudo mLACP operations. However, reversion occurs only for failed-over VLANs. The forced failover mechanism based on dynamic port-priority change cannot be used for Pseudo mLACP because all the member links will remain in the bundle state. Use the **mlacp reversion-delay** command to configure the mLACP reversion timer. Use the **mlacp load-balance force-switchover portchannel** command to configure forced VLAN switchover.

Pseudo mLACP Failover Operations

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

Note mLACP failover will not be triggered if Pseudo mLACP is not configured correctly. If the mLACP failover occurs before the peer PoA is configured with Pseudo mLACP, the failover will occur as long as the peer PoA meets the mLACP failover requirements.

- Access side link or port failure—This failure is triggered by a min-link failure. On receiving a min-link failure, all the active VLANs on the port-channel failover to the other PoA. This failover is initiated by sending a Pseudo mLACP PORT-STATE TLV message, indicating that the port state is DOWN.
- Node failure—The surviving PoA's Pseudo mLACP receives notification of node failure and initiates failover of all VLANs that were in standby mode on all shared mLAGs. After recovery, both POAs synchronize again.
- PoA uplink failure—The failing PoA signals the peer about the core isolation using the Pseudo mLACP PORT-STATE TLV, indicating that the PoA is isolated. It places all the VLANs in the blocking mode.

How to Configure ICCP Multichassis VLAN Redundancy

Configuring a Port Channel for Pseudo mLACP

Perform this task to configure a port channel for Pseudo mLACP.

Before you begin

Note The redundancy group should be configured. Redundancy group configuration for Pseudo mLACP is the same as for mLACP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *number*
4. **mlacp interchassis group** *group-id*
5. **mlacp mode active-active**
6. **mlacp load-balance primary vlan** *vlan-id*
7. **mlacp load-balance secondary vlan** *vlan-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *number* **Example:** `Router(config)# interface port-channel 1`	Configures the port channel and enters interface configuration mode.
Step 4	**mlacp interchassis group** *group-id* **Example:** `Router(config-if)# mlacp interchassis group 1`	Specifies that the port channel is an mLACP port-channel .
Step 5	**mlacp mode active-active** **Example:** `Router(config-if)# mlacp mode active-active`	Enables pseudo mLACP operations on the PoA and allows the PoA to form an LACP bundle even if the partner receives an LACP PDU from two different port channels on a dual-homed network (DHN) or dual-homed device (DHD).
Step 6	**mlacp load-balance primary vlan** *vlan-id* **Example:** `Router(config-if)# mlacp load-balance primary vlan 10,20`	Configures the list of primary VLANs that will be active and inactive on the given PoA.
Step 7	**mlacp load-balance secondary vlan** *vlan-id* **Example:** `Router(config-if)# mlacp load-balance secondary vlan 30,100`	Configures the list of secondary VLANs that will be active and inactive on the given PoA.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for ICCP Multichassis VLAN Redundancy

Example: Port Channel Configuration for Pseudo mLACP

The following example shows how to configure the port channel on the active and standby PoA for Pseudo mLACP.

Active PoA-POA1

```
Router# configure terminal
Router(config)# interface port-channel1
Router(config-if)# mlacp interchassis group 1
Router(config-if)# mlacp mode active-active
Router(config-if)# mlacp load-balance primary vlan 10,20
Router(config-if)# mlacp load-balance secondary vlan 30,100
Router(config-if)# end
```

Standby PoA-POA2

```
Router# configure terminal
Router(config)# interface port-channel1
Router(config-if)# mlacp interchassis group 1
Router(config-if)# mlacp mode active-active
Router(config-if)# mlacp load-balance primary vlan 30,100
Router(config-if)# mlacp load-balance secondary vlan 10,20
Router(config-if)# end
```

Feature Information for ICCP Multichassis VLAN Redundancy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 89: Feature Information for ICCP Multiichassis VLAN Redundancy

Feature Name	Releases	Feature Information
ICCP Multichassis VLAN Redundancy		Pseudo mLACP provides a flexible dual-homing redundancy mechanism. It uses similar principles as mLACP, but without the implementation of LACP between the PEs and CEs. The PE ports are configured in such a way that they act as if connected to a virtual device over an MC-LAG with mLACP. Ports can be placed in active/active mode with manual VLAN load balancing. The following commands were introduced or modified: **debug lacp**, **debug mvrp**, **mlacp load-balance**, **mlacp load-balance force-switchover**, **mlacp mode active-active**, **mlacp reversion-delay**, **show lacp**.

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.

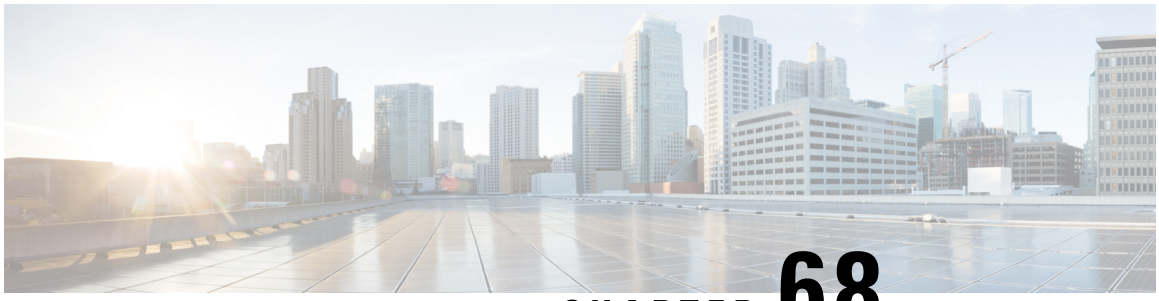
standby attachment circuit—The link that is in standby mode between the DHD and the standby PoA.

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.



CHAPTER 68

MC-LAG TCN Interworking

Multiple VLAN Registration Protocol (MVRP) is used for MAC Flushing during the Pseudowire (PW) redundancy process. However, not all Dual Homed Device (DHD) switches support MVRP for MAC flushing. MC-LAG TCN Interworking feature enables using the Multiple Spanning Tree Protocol with Topology Change Notification (MSTP TCN) scheme for MAC flushing towards the access network.

Prerequisites for MC-LAG TCN Interworking

- Ethernet Flow Points (EFPs) towards the core network as well as the access network must support the MSTP instance (creation and deletion) for sending and receiving Bridge Protocol Data Units (BPDUs).
- DHD access node(s) must support MSTP TCN.
- To enable the MAC mode for multichassis LACP (mLACP) or Pseudo mLACP (P- mLACP), mLACP sub-block must be created first.
- MSTP TCN enabled port channel interface must be compliant with High Availability (HA) synchronization (between HA Active and HA Hot Standby).

Restrictions for MC-LAG TCN Interworking

- P-mLACP mode needs to be configured before enabling MSTP TCN.
- The port channel configuration on both Point of Attachments (PoAs) must be same, including EFP IDs.
- Port channel members need not be same on PoAs.
- Each PoA may be connected to the DHD with a different number of links for the Link Aggregation Group (LAG) (and hence configured with a different value for the max-links value) variable.

- Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS) VC state (Active/Standby) are based on the Active VLAN list configuration on a PoA at any given time.

Information About MC-LAG TCN Interworking

MC-LAG TCN Interworking

Multiple Spanning Tree Protocol (MSTP) is an extension of the original STP specification. It is an IETF standard stack with a completed state machine (SM) for processing root path costs, topology change notification of the port or VLAN, and so on. MSTP uses Bridge Protocol Data Units (BPDU) to exchange information such as bridge IDs or root path costs. There are two types of BPDU in the MST stack.

- Configuration BPDU (CBPDU)
- Topology Change Notification BPDU (TCN BPDU)

Within the MST, BPDUs are exchanged regularly and enable devices to keep track of network changes and to start and stop forwarding at ports as required. MC-LAG TCN Interworking feature uses TCN BPDU to announce the changes in the network topology to access side DHD, requesting for MAC flushing. The DHD processes the MST TCN message and updates the forwarding table with appropriate outgoing interface for each destination MAC address.

MAC flushing is triggered during the following conditions:

- Pseudowire (PW) redundancy has taken place for switchover between VLANs or POAs.
- VLAN configuration has been changed by the administrator.

MSTP Topology Change Notification scheme can be configured per port-channel basis for MAC Flushing. MVRP Lite is used for MAC flushing during redundancy switchover as a default scheme.

How to Configure MC-LAG TCN Interworking

Enabling MSTP TCN Sequence

Before you begin

Note Enable P-mLACP feature before enabling MSTP TCN sequence.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *number*
4. **mlacp interchassis group** *group-id*

5. **mlacp mode active-active**
6. **mlacp mac mstp-tcn**
7. **mlacp load-balance primary vlan** *vlan-id*
8. **mlacp load-balance secondary vlan** *vlan-id*
9. **end**
10. Perform the same steps on standby POA.

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** *number* **Example:** `Device(config)# interface port-channel 1`	Configures the port channel and enters interface configuration mode.
Step 4	**mlacp interchassis group** *group-id* **Example:** `Device(config-if)# mlacp interchassis group 1`	Specifies that the port channel is an mLACP port channel.
Step 5	**mlacp mode active-active** **Example:** `Device(config-if)# mlacp mode active-active`	Enables P-mLACP operations on a PoA and allows the PoA to form an LACP bundle even if the peer receives an LACP protocol data unit (PDU) from two different port channels on a dual-homed network (DHN) or DHD.
Step 6	**mlacp mac mstp-tcn** **Example:** `Device(config-if)# mlacp mac mstp-tcn`	Enables MAC mode on port channel base.
Step 7	**mlacp load-balance primary vlan** *vlan-id* **Example:** `Device(config-if)# mlacp load-balance primary vlan 10,20`	Configures a list of primary VLANs that will be active on a given PoA.
Step 8	**mlacp load-balance secondary vlan** *vlan-id* **Example:** `Device(config-if)# mlacp load-balance secondary vlan 30,100`	Configures a list of secondary VLANs that will be standby on a given PoA.
Step 9	**end** **Example:**	Exits interface configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-if)# end`	
Step 10	Perform the same steps on standby POA.	—

Enabling MST for VLANs

SUMMARY STEPS

1. **configure terminal**
2. **spanning-tree mode mst**
3. **spanning-tree extend system-id**
4. **spanning-tree mst configuration**
5. **name** *name*
6. **revision** *version*
7. **instance** *instance-id* **vlan** *vlan-range*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**spanning-tree mode mst** **Example:** `Device(config)# spanning-tree mode mst`	Enables MST on the device.
Step 3	**spanning-tree extend system-id** **Example:** `Device(config)# spanning-tree extend system-id`	Enables the extended-system ID.
Step 4	**spanning-tree mst configuration** **Example:** `Device(config)# spanning-tree mst configuration`	Enters MST configuration submode on the system.
Step 5	**name** *name* **Example:** `Device(config-mst)# name test`	Specifies the name of an MST region
Step 6	**revision** *version* **Example:** `Device(config-mst)# revision 1`	Specifies the revision number for the MST configuration

	Command or Action	Purpose

Step 7	**instance** *instance-id* **vlan** *vlan-range*
	Example:
	`Device(config-mst)# instance 1 vlan 1-63`
	`Device(config-mst)# instance 1 vlan 20, 40`
		Maps VLANs to an MST instance.
		• *instance-id*—Range is 0 to 4094.
		• *vlan-range*—Range is 1 to 4094.
		To specify a VLAN range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 through 63 to MST instance 1.
		To specify a VLAN series, use a comma; for example, **instance 1 vlan 20, 40** maps VLANs 20 and 40 to MST instance 1.

Step 8	**exit** **Example:** `Device(config-mst)# exit`	Exits MST configuration mode and returns to global configuration mode.

Verifying MC-LAG TCN Interworking

All steps are optional and can be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show ethernet service interface** [*type number*] [**detail**]
3. **show spanning-tree detail**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables the privileged EXEC mode. Enter your password if prompted.

Step 2 **show ethernet service interface** [*type number*] [**detail**]

Example:

```
Device(config)# show ethernet service interface port 1 detail

 Interface: Port-channel1, Type: UNI
 ID:
 EVC Distribution State: Ready
 EVC Map Type: Bundling-Multiplexing
 Bridge-domains:
 Associated Service Instances:
    Service-Instance-ID CE-VLAN
    20
```

```
    40
 L2protocol pass

mLACP state: Active
```

Displays the information about mLACP enabled Ethernet interface port.

Step 3 **show spanning-tree detail**

Example:

```
Device# show spanning-tree detail

MST0 is executing the mstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 0, address f866.f2eb.7ebb
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  Current root has priority 32768, address 2834.a252.7380
  Root port is 14 (Port-channel1), cost of root path is 0
  Topology change flag not set, detected flag not set
  Number of topology changes 2 last change occurred 00:15:24 ago
          from Port-channel1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Port 14 (Port-channel1) of MST0 is root forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.14.
   Designated root has priority 32768, address 2834.a252.7380
   Designated bridge has priority 32768, address 2834.a252.7380
   Designated port id is 128.456, designated path cost 0
   Timers: message age 4, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default, Internal
   BPDU: sent 8, received 774

 MST1 is executing the mstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address f866.f2eb.7ebb
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  Current root has priority 32769, address 2834.a252.7380
  Root port is 14 (Port-channel1), cost of root path is 20000
  Topology change flag not set, detected flag not set
  Number of topology changes 3 last change occurred 00:12:04 ago
          from Port-channel1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

 Port 14 (Port-channel1) of MST1 is root forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.14.
   Designated root has priority 32769, address 2834.a252.7380
   Designated bridge has priority 32769, address 2834.a252.7380
   Designated port id is 128.456, designated path cost 0
   Timers: message age 5, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default, Internal
   BPDU: sent 8, received 775
```

Displays the STP details including TCN information.

Configuration Examples for MC-LAG TCN Interworking

Example: Enabling MSTP TCN Sequence

The following example shows how to enable the MSTP TCN sequence.

Active PoA-POA1

```
Device# configure terminal
Device(config)# interface port-channel1
Device(config-if)# mlacp interchassis group 1
Device(config-if)# mlacp mode active-active
Device(config-if)# mlacp mac mstp-tcn
Device(config-if)# mlacp load-balance primary vlan 10,20
Device(config-if)# mlacp load-balance secondary vlan 30,100
Device(config-if)# end
```

Standby PoA-POA2

```
Device# configure terminal
Device(config)# interface port-channel1
Device(config-if)# mlacp interchassis group 1
Device(config-if)# mlacp mode active-active
Device(config-if)# mlacp mac mstp-tcn
Device(config-if)# mlacp load-balance primary vlan 30,100
Device(config-if)# mlacp load-balance secondary vlan 10,20
Device(config-if)# end
```

Example: Enabling MST for VLANs

The following example shows the STP configuration for VLANs 20 and 40.

```
Device# configure terminal
Device(config)# spanning-tree mode mst
Device(config)# spanning-tree extend system-id
Device(config)# spanning-tree mst configuration
Device(config-mst)# name test
Device(config-mst)# revision 1
Device(config-mst)# instance 1 vlan 20, 40
```

Example: Configuring Redundancy and P-mLACP on Active POA

The following example shows how to configure redundancy and P-mLACP on an active POA.

```
redundancy
 mode sso
  interchassis group 4294967295
```

```
   monitor peer bfd
   member ip 88.1.1.2
   backbone interface GigabitEthernet0/0/2
   backbone interface GigabitEthernet0/0/1
   mlacp system-mac 0001.0001.0001
   mlacp system-priority 100
   mlacp node-id 1
 !
 !
interface Port-channel1
no ip address
no negotiation auto
mlacp interchassis group 4294967295
mlacp mode active-active
mlacp mac mstp-tcn
mlacp load-balance primary vlan 40
mlacp load-balance secondary vlan 20
service instance 20 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  xconnect 88.1.1.3 20 encapsulation mpls pw-class poa
backup peer 88.1.1.4 20 pw-class poa
!
service instance 40 ethernet
  encapsulation dot1q 40
  rewrite ingress tag pop 1 symmetric
  xconnect 88.1.1.3 40 encapsulation mpls pw-class poa
   backup peer 88.1.1.4 40 pw-class poa
!
interface Port-channel10
 description to-DHD
 no ip address
 mlacp interchassis group 100
 mlacp mode active-active
mlacp mac mstp-tcn
 mlacp load-balance primary vlan 100-109
 mlacp load-balance secondary vlan 110-120
  service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  xconnect 3.3.3.3 90 encapsulation mpls
!
 service instance 11 ethernet evc11_bd_201
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
  bridge-domain 201
!
 service instance 12 ethernet
  encapsulation dot1q 102
  rewrite ingress tag pop 1 symmetric
  bridge-domain 202 split-horizon
 !
 service instance 20 ethernet
  encapsulation dot1q 110
  rewrite ingress tag pop 1 symmetric
  xconnect 3.3.3.3 91 encapsulation mpls
!
service instance 21 ethernet
  encapsulation dot1q 111
  rewrite ingress tag pop 1 symmetric
  bridge-domain 211
 !
 service instance 22 ethernet
  encapsulation dot1q 112
```

```
  rewrite ingress tag pop 1 symmetric
  bridge-domain 212 split-horizon
 !
```

Example: Configuring Redundancy and P-mLACP on Standby POA

The following example shows how to configure redundancy and P-mLACP on a standby POA.

```
redundancy
 mode sso
 interchassis group 100
  monitor peer bfd
  member ip 1.1.1.1
  backbone interface GigabitEthernet8/0/10
  mlacp system-priority 100
  mlacp node-id 2


interface Port-channel1
 no ip address
 no negotiation auto
 mlacp interchassis group 4294967295
 mlacp mode active-active
 mlacp mac mstp-tcn
 mlacp load-balance primary vlan 20
 mlacp load-balance secondary vlan 40
 service instance 40  ethernet
   encapsulation dot1q 40
 rewrite ingress tag pop 1 symmetric
   xconnect 88.1.1.3 20 encapsulation mpls pw-class poa
    backup peer 88.1.1.4 20 pw-class poa
 !
 service instance 20 ethernet
   encapsulation dot1q 20
   rewrite ingress tag pop 1 symmetric
   xconnect 88.1.1.3 20 encapsulation mpls pw-class poa
    backup peer 88.1.1.4 20 pw-class poa
 !
interface Port-channel10
 description to-DHD
 no ip address
 mlacp interchassis group 100
 mlacp mode active-active
mlacp mac mstp-tcn
 mlacp load-balance primary vlan 110-120
 mlacp load-balance secondary vlan 100-109
  service instance 10 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  xconnect 3.3.3.3 90 encapsulation mpls
   !
 service instance 11 ethernet
  encapsulation dot1q 101
  rewrite ingress tag pop 1 symmetric
  bridge-domain 201
 !
 service instance 12 ethernet
  encapsulation dot1q 102
  rewrite ingress tag pop 1 symmetric
```

```
  bridge-domain 202 split-horizon
 !
 service instance 20 ethernet
  encapsulation dot1q 110
  rewrite ingress tag pop 1 symmetric
  xconnect 3.3.3.3 91 encapsulation mpls
   !
service instance 21 ethernet
  encapsulation dot1q 111
  rewrite ingress tag pop 1 symmetric
  bridge-domain 211
 !
 service instance 22 ethernet
  encapsulation dot1q 112
  rewrite ingress tag pop 1 symmetric
  bridge-domain 212 split-horizon
 !
End
```

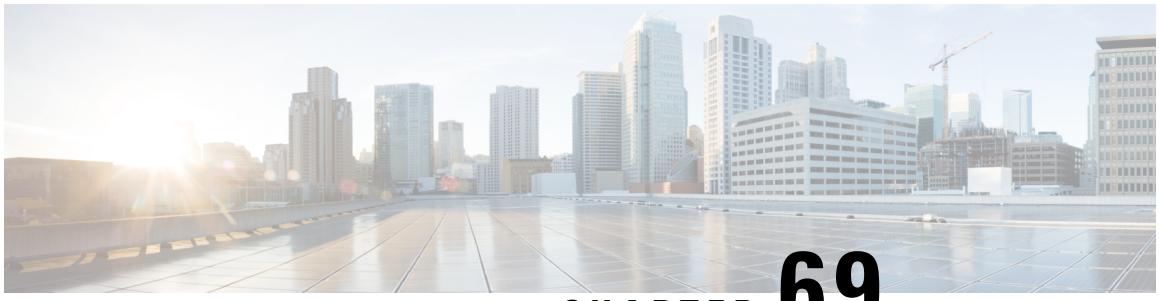
Feature Information for MC-LAG TCN Interworking

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 90: Feature Information for MC-LAG TCN Interworking

Feature Name	Releases	Feature Information
MC-LAG TCN Interworking	Cisco IOS XE Release 3.17S	Multiple VLAN Registration Protocol (MVRP) is used for MAC Flushing during the Pseudowire (PW) redundancy process. However, not all Dual Homed Device (DHD) switches support MVRP for MAC flushing. MC-LAG TCN Interworking feature enables using the Multiple Spanning Tree Protocol with Topology Change Notification (MSTP TCN) scheme for MAC Flushing towards the access network. The following commands were introduced or modified: **mlacp mac mstp-tcn**, **show ethernet service**, **show spanning-tree detail**



CHAPTER 69

Configuring ITU-T Y.1731 Fault Management Functions in IEEE CFM

This document describes the implementation of the ITU-Y.1731 fault management functions Ethernet Alarm Indication Signal (ETH-AIS) and Ethernet Remote Defect Indication (ETH-RDI) as part of the IEEE Ethernet Connectivity Fault Management (CFM) protocol.

Prerequisites for Configuring ITU-T Y.1731 Fault Management Functions

Business Requirements

- Business and service policies have been established.
- Network topology and network administration have been evaluated.

Technical Requirements

- CFM must be configured and enabled for Y.1731 fault management features to function.
- A server maintenance endpoint (SMEP) is needed to support the ETH-AIS function.
- Maintenance intermediate points (MIPs) must be configured to support AIS messages; they are generated only on an interface on which a MIP is configured.

Restrictions for Configuring ITU-T Y.1731 Fault Management Functions

- Because of a port-ASIC hardware limitation, IEEE CFM cannot coexist with the Per VLAN Spanning Tree (PVST) protocol, and IEEE CFM cannot operate with the following line cards on the same system:
  - FI_WS_X6196_RJ21
  - FI_WS_X6196_RJ45
  - FI_WS_X6548_RJ21
  - FI_WS_X6548_RJ45
- CFM loopback messages are not confined within a maintenance domain according to their maintenance level. The impact of not having CFM loopback messages confined to their maintenance levels occurs at these levels:
  - Architecture--CFM layering is violated for loopback messages.
  - Deployment--A user may misconfigure a network and have loopback messages succeed.
  - Security--A malicious device that recognizes devices' MAC addresses and levels may explore a network topology that should be transparent.
- Routed interfaces are supported only in Cisco IOS Release 12.4(11)T.
- IEEE CFM is not fully supported on a Multiprotocol Label Switching (MPLS) provider edge (PE) device. There is no interaction between IEEE CFM and an Ethernet over MPLS (EoMPLS) pseudowire. A CFM packet can be transparently passed like regular data packets only via pseudowire, with the following restriction:
  - For policy feature card (PFC)-based EoMPLS, which uses a Cisco Catalyst LAN card as the MPLS uplink port, a CFM packet can be transparently passed via an EoMPLS pseudowire the same way regular data packets are passed. The EoMPLS endpoint interface, however, cannot be a maintenance endpoint (MEP) or an MIP, although a CFM MEP or MIP can be supported on regular Layer 2 switchport interfaces.
- CFM configuration is not supported on an EtherChannel in FastEthernet Channel (FEC) mode.

Information About Configuring ITU-T Y.1731 Fault Management Functions

Continuity Check Messages

CFM continuity check messages (CCMs) are multicast heartbeat messages exchanged periodically among MEPs. CCMs allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CCMs are confined to a domain.

For more information about CCMs, see the "Continuity Check Messages" section of the "Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network" configuration module.

Server MEPs

Server MEPs (SMEPs) are virtual MEPs that perform two functions--server layer termination for CFM maintenance associations defined at a link or at the transport layer and server-Ethernet adaptation. When a SMEP detects a defect at the server layer, it issues frames containing ETH-AIS information.

Defect Conditions Detected by a MEP

The defect conditions that a MEP detects and subsequently acts upon are the following:

- AIS condition--A MEP receives an AIS frame.
- Dying gasp--An unrecoverable and vendor-specific condition. Dying gasp is generated in the following conditions:
  - Administratively disabling 802.3ah
  - Link down caused by administration down
  - Power failure
  - Reload

Note Administratively disabling 802.3ah does not disrupt traffic and should not generate an AIS. If a Reason field is empty, however, disabling always generates an AIS when Cisco routers and non-Cisco routers are interworking.

A notification about the defect condition may be sent immediately and continuously.

- Loss of continuity (LOC) condition--A MEP stops receiving CCMs from a peer MEP. An LOC condition is a MEP down error.

LOC results when a remote MEP lifetime timer expires and causes an AIS condition for the local MEP. The LOC condition is cleared when connectivity is restored.

- Mismerge condition--A CCM with a correct maintenance level but incorrect maintenance ID indicates that frames from a different service instance are merged with the service instance represented by the receiving MEP's maintenance ID. A mismerge condition is a cross-connect error.
- RDI condition--A MEP receives a CCM with the RDI field set.
- Signal fail condition--Declared by a MEP or the server layer termination function to notify the SMEP about a defect condition in the server layer. Signal fail conditions are as follows:
  - Configuration error
  - Cross-connect error
  - LOC
  - Loop error
  - MEP missing
  - MEP unknown (same as unexpected MEP)

Signal fail conditions cause AIS defect conditions for the MEP, resulting in the MEP receiving an AIS frame.

A MEP that detects a signal fail condition sends AIS frames to each of the client layer or sublayer maintenance associations.

- Unexpected MEP condition--A CCM with a correct maintenance level, correct maintenance ID, and an unexpected maintenance point ID (MPID) that is the same as the receiving MEP's MPID. An unexpected MEP condition is either a cross-check error or a configuration error.

Determination of an unexpected MPID is possible when a MEP maintains a list of its peer MPIDs. Peer MPIDs must be configured on each MEP during provisioning.

ETH-AIS Function

The ETH-AIS function suppresses alarms when a defect condition is detected at either the server layer or the server sublayer (virtual MEP). Transmission of frames carrying ETH-AIS information can be either enabled or disabled on either a MEP or a SMEP and can be sent at the client maintenance level by either a MEP or SMEP when a defect condition is detected.

SMEPs monitor the entire physical link so that an AIS is generated for each VLAN or server on the network. MEPs monitor VLANs, Ethernet virtual circuits (EVCs), and SMEPs where link up or link down and 802.3ah interworking are supported. A MEP that detects a connectivity fault at a specific level multicasts an AIS in the direction opposite the detected failure at the client maintenance association (MA) level.

An AIS causes a receiving MEP to suppress traps to prevent the network management system (NMS) from receiving an excessive number of redundant traps and also so that clients are asynchronously informed about faults.

In a point-to-point topology, a MEP has a single peer MEP and there is no ambiguity regarding the peer MEP for which it should suppress alarms when it receives ETH-AIS information.

In a multipoint Ethernet topology, a MEP that receives a frame with ETH-AIS information cannot determine which remote peer lost connectivity. The MEP also cannot determine the associated subset of peer MEPs for which it should suppress alarms because the ETH-AIS information does not include that MEP information. Because the MEP cannot determine the affected peer MEPs, it suppresses alarms for all peer MEPs whether or not there is connectivity.

Due to independent restoration capabilities within Spanning Tree Protocol (STP) environments, ETH-AIS is not expected to be applied in these environments; however, ETH-AIS transmission is configurable in STP environments by a network administrator.

ETH-AIS Transmission Reception and Processing

Only a MEP or a SMEP can be configured to send frames with ETH-AIS information. When a MEP detects a defect condition, it immediately begins transmitting frames with ETH-AIS information at the configured client maintenance level, which is the level at which the MIP is configured on the interface. Frames are transmitted to peer MEPs in the direction opposite the fault. The first AIS frame must always be transmitted immediately following the detection of a defect condition, but thereafter frames are transmitted at a frequency based on the configured AIS transmission period. The transmitting MEP continues to transmit frames with ETH-AIS information until the defect condition is removed. The period flag in the frame's header indicates the transmission interval. The default is that a MEP clears a defect condition only if no AIS frames are received within a time period equal to 3.5 times the configured transmission interval.

Note An AIS transmission period of one second is recommended; however, an AIS transmission period of one minute is supported to enable ETH-AIS across all VLANs supported by IEEE CFM.

When a MEP receives a frame with ETH-AIS information, it examines the frame to ensure that the maintenance association level corresponds to its own maintenance association level. The MEP detects the AIS condition and suppresses loss-of-continuity alarms associated with all its peer MEPs. Peer MEPs can resume generating loss-of-continuity alarms only when the receiving MEP exits the AIS condition.

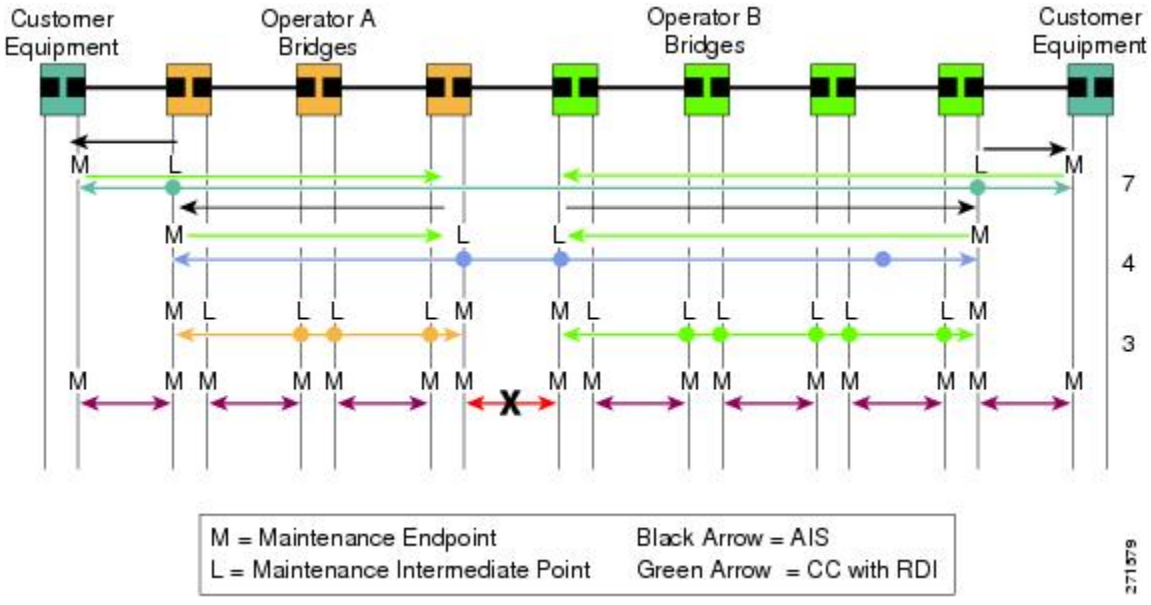
The client layer or client sublayer may consist of multiple maintenance associations that should also be notified to suppress alarms when either a server layer or server sublayer MEP detects a defect condition. The first AIS frame for all client layer or sublayer maintenance associations must be transmitted within one second after the defect condition is detected.

AIS and 802.3ah Interworking

The following conditions impact SMEP AIS conditions:

- By default, link down events cause the SMEP to enter the AIS condition and generate AIS frames for all services at the immediate client maintenance association level.
- Link up events cause the SMEP to exit the AIS state and stop generating AIS frames.
- Local fault detection results from dying gasp, link fault, or critical 802.3ah Remote Fault Indication (RFI). When 802.3ah is reestablished, the SMEP exits the AIS state and stops generating AIS frames.
- Local fault detection due to crossing of a high threshold with a configurable action of error disabling the interface.
- RFI received from a dying gasp, link fault, or critical event.

If a detected fault is due to dying gasp, the link goes down in both directions, creating AIS and RDI frame flow as shown in the figure below.



ETH-RDI Function

The ETH-RDI function is used by a MEP to communicate to its peer MEPs that a defect condition has been encountered. ETH-RDI is used only when ETH-CC transmission is enabled.

ETH-RDI has the following two applications:

- Single-ended fault management--A receiving MEP detects an RDI defect condition, which is correlated with other defect conditions in the MEP and may become the cause of a fault. If ETH-RDI information is not received by a single MEP, there are no defects in the entire MA.
- Contribution to far-end performance monitoring--A defect condition in the far end is used as an input to the performance monitoring process.

A MEP in a defect condition transmits CCMs with ETH-RDI information. A MEP that receives a CCM examines it to ensure that its maintenance association level corresponds to its configured maintenance association level and detects the RDI condition if the RDI field is set. The receiving MEP sets the RDI field in CCMs for the duration of a defect condition, and if the MEP is enabled for CCM transmission, transmits CCMs based on the configured transmission interval. When the defect condition clears, the MEP clears the RDI field in CCMs for subsequent transmissions.

In a point-to-point Ethernet connection, a MEP can clear an RDI condition when it receives the first CCM with the RDI field cleared from its peer MEP. In a multipoint Ethernet connection, a MEP cannot determine the peer MEP with the default condition and can clear an RDI condition only when it receives a CCM with the RDI field cleared from each of its peer MEPs.

The ETH-RDI function is part of continuity checking and is enabled by default. For more information about continuity checking, see the "Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network" configuration module.

How to Configure ITU-T Y.1731 Fault Management Functions

ETH-AIS and ETH-RDI both are enabled by default when CFM is configured, but each can also be manually enabled by a separate command during CFM configuration. Perform these tasks to either disable or enable the functions.

Disabling the ETH-AIS Function

Perform this task to disable the ETH-AIS function.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm ais link-status global**
4. **disable**
5. **exit**
6. **ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]
7. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]]
8. **no ais** [**expiry-threshold** | **level** | **period** | **suppress-alarms**]

9. **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	**ethernet cfm ais link-status global** **Example:** `Device(config)# ethernet cfm ais link-status global`	Globally enables AIS generation and enters CFM SMEP AIS configuration mode.
Step 4	**disable** **Example:** `Device(config-ais-link-cfm)# disable`	Disables AIS transmission.
Step 5	**exit** **Example:** `Device(config-ais-link-cfm)# exit`	Returns the CLI to global configuration mode.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain PROVIDERDOMAIN level 4`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 7	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]] **Example:** `Device(config-ecfm)# service customer101provider evc customer101provider@101 vlan 101`	Configures a maintenance association within a maintenance domain and enters Ethernet CFM service configuration mode.
Step 8	**no ais** [**expiry-threshold** | **level** | **period** | **suppress-alarms**] **Example:**	Disables the AIS function for a specific maintenance association.

	Command or Action	Purpose
	`Device(config-ecfm-srv)# no ais`	
Step 9	**end** **Example:** `Device(config-ecfm-srv)# end`	Returns the CLI to privileged EXEC mode.

Enabling ETH-AIS for a Single Interface SMEP and Disabling ETH-AIS for All Other Ports

Perform this task to manually enable the ETH-AIS function.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**]
4. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]]
5. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
6. **ais** [**expiry-threshold** *threshold* | **level** *level-id* | **period** *seconds*| **suppress-alarms**]
7. **ais** [**expiry-threshold** *threshold* | **level** *level-id* | **period** *seconds*| **suppress-alarms**]
8. **exit**
9. **service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]]
10. **continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**]
11. **ethernet cfm ais link-status global**
12. disable
13. **interface** *type number*
14. **ethernet oam remote-loopback** {**supported** | **timeout** *seconds*}
15. **ethernet cfm mip level** *level-id* [**vlan** {*vlan-id*| *vlan-id - vlan-id*| **,** *vlan-id - vlan-id*}]
16. **ethernet cfm ais link-status** [**level** *level-id*| **period** *seconds*]
17. **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.

	Command or Action	Purpose
Step 3	**ethernet cfm domain** *domain-name* **level** *level-id* [**direction outward**] **Example:** `Device(config)# ethernet cfm domain PROVIDERDOMAIN level 4`	Defines a CFM maintenance domain at a particular maintenance level and enters Ethernet CFM configuration mode.
Step 4	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]] **Example:** `Device(config-ecfm)# service customer101provider evc customer101provider@101 vlan 101`	Configures a maintenance association within a maintenance domain and enters Ethernet CFM service configuration mode.
Step 5	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:** `Device(config-ecfm-srv)# continuity-check`	Enables the transmission of CCMs.
Step 6	**ais** [**expiry-threshold** *threshold* | **level** *level-id* | **period** *seconds*| **suppress-alarms**] **Example:** `Device(config-ecfm-srv)# ais period 1`	Enables the AIS function for a specific maintenance association.
Step 7	**ais** [**expiry-threshold** *threshold* | **level** *level-id* | **period** *seconds*| **suppress-alarms**] **Example:** `Device(config-ecfm-srv)# ais level 7`	Enables the AIS function for a specific maintenance association.
Step 8	**exit** **Example:** `Device(config-ecfm-srv)# exit`	Returns the CLI to Ethernet CFM configuration mode.
Step 9	**service** {*ma-name* | *ma-num* | **vlan-id** *vlan-id* | **vpn-id** *vpn-id*} [**port** | **vlan** *vlan-id* [**direction down**]] **Example:** `Device(config-ecfm)# service customer110provider evc customer110provider@110 vlan 110`	Configures a maintenance association within a maintenance domain and enters Ethernet CFM service configuration mode.
Step 10	**continuity-check** [**interval** *time* | **loss-threshold** *threshold* | **static rmep**] **Example:**	Enables the transmission of CCMs.

	Command or Action	Purpose
	`Device(config-ecfm-srv)# continuity-check`	
Step 11	**ethernet cfm ais link-status global** **Example:** `Device(config-ecfm-srv)# ethernet cfm ais link-status global`	Globally enables AIS generation and places the CLI in CFM SMEP AIS configuration mode (config-ais-link-cfm) to configure AIS commands for a SMEP.
Step 12	disable **Example:** `Device(config-ais-link-cfm)# disable`	Disables the generation of AIS frames resulting from a link-status change.
Step 13	**interface** *type number* **Example:** `Device(config-ais-link-cfm)# interface ethernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 14	**ethernet oam remote-loopback** {**supported** | **timeout** *seconds*} **Example:** `Device(config-if)# ethernet oam remote-loopback supported`	Enables the support of Ethernet OAM remote loopback operations on an interface or sets a remote loopback timeout period.
Step 15	**ethernet cfm mip level** *level-id* [**vlan** {*vlan-id*| *vlan-id - vlan-id*| **,** *vlan-id - vlan-id*}] **Example:** `Device(config-if)# ethernet cfm mip level 4 vlan 101`	Provisions a MIP at a specified maintenance level on an interface.
Step 16	**ethernet cfm ais link-status** [**level** *level-id*| **period** *seconds*] **Example:** `Device(config-if)# ethernet cfm ais link-status`	Enables AIS generation from a SMEP.
Step 17	**end** **Example:** `Device(config-if)# end`	Returns the CLI to privileged EXEC mode.

Configuration Examples for Configuring ITU-T Y.1731 Fault Management Functions

Example: Enabling IEEE CFM on an Interface

The following example shows how to enable IEEE CFM on an interface:

```
!
ethernet cfm domain ServiceProvider level 4
mep archive-hold-time 60
service MetroCustomer1 vlan 100
!
ethernet cfm domain OperatorA level 1
mep archive-hold-time 65
service MetroCustomer1OpA vlan 100
!
ethernet cfm enable
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 60
!
interface gigabitethernet3/0
ethernet cfm mip level 1
!
interface gigabitethernet4/0
ethernet cfm mip level 4
ethernet cfm mep level 1 mpid 102 vlan 100
!
ethernet cfm cc enable level 1 vlan 100
ethernet cfm cc level any vlan any interval 20 loss-threshold 3
```

Example: Enabling AIS

The following example shows how to enable AIS:

```
!
ethernet cfm domain PROVIDER_DOMAIN level 4
 service customer101provider evc customer101provider@101 vlan 101
  continuity-check
  ais period 1
  ais level 7
 service customer110provider evc customer110provider@110 vlan 110
  continuity-check
!
ethernet cfm ais link-status global
 disable
!
!
interface Ethernet 0/1
 no ip address
 ethernet oam remote-loopback supported
 ethernet oam
 ethernet cfm mip level 4 vlan 1,101,110
 ethernet cfm ais link-status
!
```

Example: Show Commands Output

The following sample output from the **show ethernet cfm maintenance-point local detail** command shows the settings for the local MEP:

```
Device# show ethernet cfm maintenance-points local detail

MEP Settings:
-------------
MPID: 2101
DomainName: PROVIDERDOMAIN
Level: 4
Direction: I
Vlan: 101
Interface: Et0/1
CC-Status: Enabled
MAC: aabb.cc03.8410
Defect Condition: AIS
presentRDI: TRUE
AIS-Status: Enabled
AIS Period: 1000(ms)
AIS Expiry Threshold: 3.5
Level to transmit AIS: Default
Suppress Alarm configuration: Enabled
Suppressing Alarms: Yes
```

The following sample output from the **show ethernet cfm smep** command shows the settings for a SMEP:

```
Device# show ethernet cfm smep
SMEP Settings:
--------------
Interface: Ethernet0/0
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: 4
Defect Condition: No Defect
```

The following sample output from the **show ethernet cfm smep interface** command shows the settings for a specific interface on a SMEP:

```
Device# show ethernet cfm smep interface ethernet 0/1
SMEP Settings:
--------------
Interface: Ethernet0/1
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: No Defect
Router#
```

The following sample output from the **show ethernet cfm errors** command shows the Ethernet CFM errors on a device:

```
Device# show ethernet cfm errors
Level    Vlan    MPID    Remote MAC        Reason         Service ID
5        102     -       aabb.cc00.ca10    Receive AIS    service test
```

The following sample output from the **show ethernet cfm maintenance-points remote detail** command shows the detailed information about a specific remote MEP:

```
Device# show ethernet cfm maintenance-points remote detail mpid 66
MAC Address: aabb.cc00.ca10
Domain/Level: PROVIDERDOMAIN/4
EVC: test
MPID: 66 (Can ping/traceroute)
Incoming Port(s): Ethernet0/2
CC Lifetime(sec): 75
Age of Last CC Message(sec): 8
Receive RDI: TRUE
Frame Loss: 0%
CC Packet Statistics: 2/0 (Received/Error)
R1#MAC Address: aabb.cc00.ca10
Domain/Level: PROVIDERDOMAIN/4
EVC: test
MPID: 66 (Can ping/traceroute)
Incoming Port(s): Ethernet0/2
CC Lifetime(sec): 75
Age of Last CC Message(sec): 8
Receive RDI: TRUE
Frame Loss: 0%
CC Packet Statistics: 2/0 (Received/Error)
```

Additional References

Related Documents

Related Topic	Document Title
IEEE CFM	"Configuring IEEE Standard-Compliant Ethernet CFM in a Service Provider Network"
Using OAM	"Using Ethernet Operations, Administration, and Maintenance"
IEEE CFM and Y.1731 commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Standards

Standard	Title
IEEE 802.1ag	*802.1ag - Connectivity Fault Management*
IEEE 802.3ah	*Ethernet in the First Mile*
ITU-T	*ITU-T Y.1731 OAM Mechanisms for Ethernet-Based Networks*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

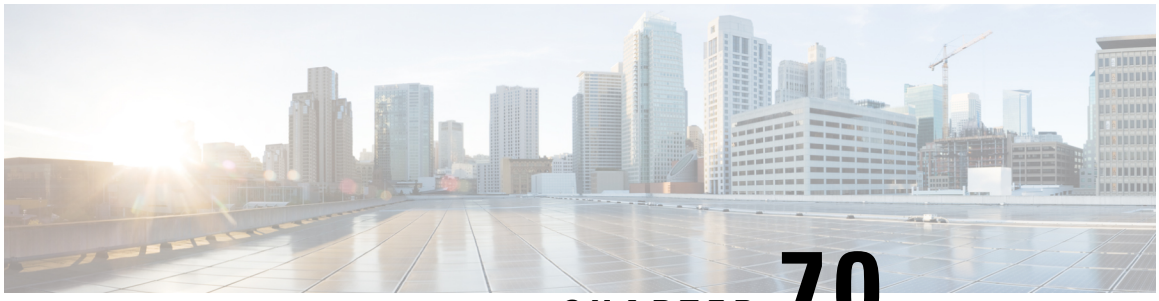
Feature Information for Configuring ITU-T Y.1731 Fault Management Functions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 91: Feature Information for Configuring ITU-T Y.1731 Fault Management Functions

Feature Name	Releases	Feature Information
Configuring ITU-T Y.1731 Fault Management Functions	15.0(1)XA 12.2(33)SRE 15.1(1)T Cisco IOS XE Release 3.8S	The ITU-Y.1731 Fault Management Functions feature adds to IEEE CFM the ETH-AIS and ETH-RDI functions for fault detection, fault verification, and fault isolation in large MANs and WANs. The following commands were introduced or modified: **ais**, **clear ethernet cfm ais**, **disable**(CFM-AIS-link), **ethernet cfm ais link-status**, **ethernet cfm ais link-status global**, **level**(cfm-ais-link), **period**(cfm-ais-link), **show ethernet cfm errors**, **show ethernet cfm maintenance-points local**, **show ethernet cfm maintenance-points remote detail**, **show ethernet cfm smep**.



CHAPTER 70

Configuring IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

This module describes how to configure an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation to gather the following performance measurements for Ethernet service:

- Ethernet Delay
- Ethernet Delay Variation
- Ethernet Frame Loss Ratio

Prerequisites for ITU-T Y.1731 Operations

IEEE-compliant Connectivity Fault Management (CFM) must be configured and enabled for Y.1731 performance monitoring to function.

Note Y1731 is supported on Port Channel interfaces.

Restrictions for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

- SNMP is not supported for reporting threshold events or collecting performance statistics for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operations.

  SNMP is partially supported; the results for DM/LM can be polled for some attributes. However MIB support for all parameters is not supported.

- Continuity Check Message (CCM)-based dual-ended Ethernet frame loss operations are not supported.

- In a single-ended Ethernet operation, performance measurement statistics can be retrieved only at the device on which the sender Ethernet Connectivity Fault Management (CFM) Maintenance End Point (MEP) is configured.
- To avoid losing the CoS value configured on the frames, do not configure **rewrite** on the EFPs throughout the Layer2 circuit. The CoS value is preserved, if the Y.1731 frames are marked with specific CoS value.
- CFM over cross-connect on the routers works only if the **control-word** is configured. To start DM timestamping, switch ON the control-word if the remote end is not switched ON.
- To avoid errors in RX and TX timestamping, ensure to have Y1731 sender as primary PTP, and the Y1731 responder as subordinate PTP.
- Reconfigure IP SLA Y1731 while doing online insertion removal (OIR) of IM or router reload because local MEP is deleted during the course.
- A delay may be observed after issuing the **ip sla schedule** command after a reload of the router is performed, to populate with the Y.1731 PM measurements.
- The dot1q tag contains class of service (CoS) bits, which are used by IPSLA Y.1731 PM session to test delay or loss of packets with a specific CoS. This CoS cannot be a non-zero value when using EPM over untagged EFPs.

How to Configure IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Configuring a Dual-Ended Ethernet Delay or Delay Variation Operation

Perform the tasks for configuring a dual-ended operation in the order presented.

Note To remove the MEP configurations in an already-configured dual-ended operation, always remove the MEPs in the reverse order in which they were configured. That is, remove the scheduler first, then the threshold monitoring configuration, and then the sender MEP configuration on the source device before removing the scheduler, proactive threshold monitoring, and receiver MEP configuration on the destination device.

Configuring a Receiver MEP on the Destination Device

Before you begin

Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip sla** *operation-number*
4. **ethernet y1731 delay receive 1DM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} **cos** *cos* {**mpid** *source-mp-id* | **mac-address** *source-address*}
5. **aggregate interval** *seconds*
6. **distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,***boundary*]
7. **frame offset** *offset-value*
8. **history interval** *intervals-stored*
9. **max-delay** *milliseconds*
10. **owner** *owner-id*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Router(config-term)# ip sla 501`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 delay receive 1DM domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} **cos** *cos* {**mpid** *source-mp-id* | **mac-address** *source-address*} **Example:** `Router(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101`	Begins configuring the receiver on the responder and enters IP SLA Y.1731 delay configuration mode. • The *source-mp-id* or *source-address* configured by this command corresponds to that of the MEP being configured. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.

	Command or Action	Purpose
Step 6	**distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,***boundary*] **Example:** `Router(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000,10000,15000,20000,-1`	(Optional) Specifies measurement type and configures bins for statistics distributions kept.
Step 7	**frame offset** *offset-value* **Example:** `Router(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets the value for calculating delay variation rates.
Step 8	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 9	**max-delay** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# max-delay 5000`	(Optional) Sets the amount of time an MEP waits for a frame.
Step 10	**owner** *owner-id* **Example:** `Router(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 11	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring the Sender MEP on the Source Router

Before you begin

- Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.
- The receiver MEP must be configured, including proacive threshold monitoring, and scheduled before you configure the sender MEP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla operation-number**
4. **ethernet y1731 delay 1DM domain domain-name** {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **aggregate interval** *seconds*
6. **frame interval** *milliseconds*
7. **frame size** *bytes*
8. **history interval** *intervals-stored*
9. **owner** *owner-id*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip sla operation-number** **Example:** `Router(config)# ip sla 500`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 delay 1DM domain domain-name** {**evc** *evc-id*	**vlan** *vlan-id*} {**mpid** *target-mp-id*	**mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id*	**mac-address** *source-address*}}	Begins configuring a dual-ended Ethernet delay operation and enters IP SLA Y.1731 delay configuration mode. **Note** The session with mac-address will not be inactivated when there is CFM error.

	Command or Action	Purpose
	Example: `Router(config-ip-sla)# ethernet y1731 delay 1DM domain xxx evc yyy mpid 101 cos 3 source mpid 100`	
Step 5	**aggregate interval** *seconds* **Example:** `Router(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 6	**frame interval** *milliseconds* **Example:** `Router(config-sla-y1731-delay)# frame interval 100`	(Optional) Sets the gap between successive frames.
Step 7	**frame size** *bytes* **Example:** `Router(config-sla-y1731-delay)# frame size 64`	(Optional) Sets the padding size for frames.
Step 8	**history interval** *intervals-stored* **Example:** `Router(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 9	**owner** *owner-id* **Example:** `Router(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 10	**end** **Example:** `Router(config-sla-y1731-delay)# end`	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring a Sender MEP for a Single-Ended Ethernet Delay or Delay Variation Operation

Perform this task to configure a sender MEP on the source device.

Before you begin

- Time synchronization is required between the source and destination devices in order to provide accurate one-way delay (latency) or delay-variation measurements. Configure either Precision Time Protocol (PTP) or Network Time Protocol (NTP) on both the source and destination devices.

Note To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet y1731 delay** {**DMM** | **DMMv1**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **clock sync**
6. **aggregate interval** *seconds*
7. **distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,**boundary*]
8. **frame interval** *milliseconds*
9. **frame offset** *offset-value*
10. **frame size** *bytes*
11. **history interval** *intervals-stored*
12. **max-delay** *milliseconds*
13. **owner** *owner-id*
14. **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	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 10`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 delay** {**DMM** | **DMMv1**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **cos** *cos* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} **Example:** `Device(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 4 source mpid 100`	Begins configuring a single-ended Ethernet delay operation and enters IP SLA Y.1731 delay configuration mode. • To configure concurrent operations, use the **DMMv1** keyword with this command. Repeat the preceding two steps to each concurrent operation, to be added to a single IP SLA operation number. Concurrent operations are supported for a given EVC, CoS, and remote MEP combination, or for multiple MEPs for a given multipoint EVC. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**clock sync** **Example:** `Device(config-sla-y1731-delay)# clock sync`	(Optional) Indicates that the end points are synchronized and thus allows the operation to calculate one-way delay measurements.
Step 6	**aggregate interval** *seconds* **Example:** `Device(config-sla-y1731-delay)# aggregate interval 900`	(Optional) Configures the length of time during which the performance measurements are conducted and the results stored.
Step 7	**distribution** {**delay** | **delay-variation**} **one-way** *number-of-bins boundary*[**,...,***boundary*] **Example:** `Device(config-sla-y1731-delay)# distribution delay-variation one-way 5 5000, 10000,15000,20000,-1`	(Optional) Specifies measurement type and configures bins for statistics distributions kept.
Step 8	**frame interval** *milliseconds* **Example:**	(Optional) Sets the gap between successive frames.

	Command or Action	Purpose
	`Device(config-sla-y1731-delay)# frame interval 100`	
Step 9	**frame offset** *offset-value* **Example:** `Device(config-sla-y1731-delay)# frame offset 1`	(Optional) Sets value for calculating delay variation values.
Step 10	**frame size** *bytes* **Example:** `Device(config-sla-y1731-delay)# frame size 32`	(Optional) Configures padding size for frames.
Step 11	**history interval** *intervals-stored* **Example:** `Device(config-sla-y1731-delay)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 12	**max-delay** *milliseconds* **Example:** `Device(config-sla-y1731-delay)# max-delay 5000`	(Optional) Sets the amount of time an MEP waits for a frame.
Step 13	**owner** *owner-id* **Example:** `Device(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 14	**end** **Example:** `Device(config-sla-y1731-delay)# end`	Exits to privileged EXEC mode.

What to do next

To add proactive threshold conditions and reactive triggering for generating traps, see the "Configuring Proactive Threshold Monitoring" module of the *IP SLAs Configuration Guide*.

When you are finished configuring proactive threshold monitoring for this operation, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Configuring a Sender MEP for a Single-Ended Ethernet Frame Loss Ratio Operation

Note To display information about remote (target) MEPs on destination devices, use the **show ethernet cfm maintenance-points remote** command.

Perform this task to configure a sender MEP on the source device.

Before you begin

- Class of Service (CoS)-level monitoring must be enabled on MEPs associated to the Ethernet frame loss operation by using the **monitor loss counter** command on the devices at both ends of the operation. See the *Cisco IOS Carrier Ethernet Command Reference* for command information. See the "Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations" section for configuration information.

Note Cisco IOS Y.1731 implementation allows monitoring of frame loss for frames on an EVC regardless of the CoS value (any CoS or Aggregate CoS cases). See the "Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations" section for configuration information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}}
5. **aggregate interval** *seconds*
6. **availability algorithm** {**sliding-window** | **static-window**}
7. **frame consecutive** *value*
8. **frame interval** *milliseconds*
9. **history interval** *intervals-stored*
10. **owner** *owner-id*
11. **exit**
12. **exit**
13. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sla** *operation-number* **Example:** `Device(config-term)# ip sla 11`	Begins configuring an IP SLAs operation and enters IP SLA configuration mode.
Step 4	**ethernet y1731 loss** {**LMM** | **SLM**} [**burst**] **domain** *domain-name* {**evc** *evc-id* | **vlan** *vlan-id*} {**mpid** *target-mp-id* | **mac-address** *target-address*} **CoS** *CoS* {**source** {**mpid** *source-mp-id* | **mac-address** *source-address*}} **Example:** `Device(config-ip-sla)# ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 CoS 4 source mpid 23`	Begins configuring a single-ended Ethernet frame loss ratio operation and enters IP SLA Y.1731 loss configuration mode. • To configure concurrent operations, use the **SLM** keyword with this command. Repeat the preceding two steps to configure each concurrent operation to be added to a single IP SLA operation number. Concurrent operations are supported for a given EVC, CoS, and remote-MEP combination, or for multiple MEPs for a given multipoint EVC. **Note** The session with mac-address will not be inactivated when there is CFM error.
Step 5	**aggregate interval** *seconds* **Example:** `Device(config-sla-y1731-loss)# aggregate interval 900`	(Optional) Configures the length of time during which performance measurements are conducted and the results stored.
Step 6	**availability algorithm** {**sliding-window** | **static-window**} **Example:** `Device(config-sla-y1731-loss)# availability algorithm static-window`	(Optional) Specifies availability algorithm used.
Step 7	**frame consecutive** *value* **Example:** `Device(config-sla-y1731-loss)# frame consecutive 10`	(Optional) Specifies number of consecutive measurements to be used to determine availability or unavailability status.

	Command or Action	Purpose
Step 8	**frame interval** *milliseconds* **Example:** `Device(config-sla-y1731-loss)# frame interval 100`	(Optional) Sets the gap between successive frames.
Step 9	**history interval** *intervals-stored* **Example:** `Device(config-sla-y1731-loss)# history interval 2`	(Optional) Sets the number of statistics distributions kept during the lifetime of an IP SLAs Ethernet operation.
Step 10	**owner** *owner-id* **Example:** `Device(config-sla-y1731-delay)# owner admin`	(Optional) Configures the owner of an IP SLAs operation.
Step 11	**exit** **Example:** `Device(config-sla-y1731-delay)# exit`	Exits to IP SLA configuration mode.
Step 12	**exit** **Example:** `Device(config-ip-sla)# exit`	Exits to global configuration mode.
Step 13	**exit** **Example:** `Device(config)# exit`	Exits to privileged EXEC mode.

What to do next

When you are finished configuring this MEP, see the "Scheduling IP SLAs Operations" section to schedule the operation.

Scheduling IP SLAs Operations

Before you begin

- All IP Service Level Agreements (SLAs) operations to be scheduled must be already configured.

- The frequency of all operations scheduled in a multioperation group must be the same.
- The list of one or more operation ID numbers to be added to a multioperation group must be limited to a maximum of 125 characters in length, including commas (,).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]
   - **ip sla group schedule** *group-operation-number operation-id-numbers* {**schedule-period** *schedule-period-range* | **schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm* [:*ss*]}]
4. **end**
5. **show ip sla group schedule**
6. **show ip sla configuration**

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	Enter one of the following commands: • **ip sla schedule** *operation-number* [**life** {**forever**	*seconds*}] [**start-time** {[*hh*:*mm*:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**] • **ip sla group schedule** *group-operation-number operation-id-numbers* {**schedule-period** *schedule-period-range*	**schedule-together**} [**ageout** *seconds*] **frequency** *group-operation-frequency* [**life** {**forever**	*seconds*}] [**start-time** {*hh*:*mm* [:*ss*] [*month day*	*day month*]	**pending**	**now**	**after** *hh*:*mm* [:*ss*]}] **Example:** `Device(config)# ip sla schedule 10 life forever start-time now`	• Configures the scheduling parameters for an individual IP SLAs operation. • Specifies an IP SLAs operation group number and the range of operation numbers for a multioperation scheduler.

	Command or Action	Purpose

	`Device(config)# ip sla group schedule 10 schedule-period frequency`
	
	`Device(config)# ip sla group schedule 1 3,4,6-9 life forever start-time now`
	
	`Device(config)# ip sla schedule 1 3,4,6-9 schedule-period 50 frequency range 80-100`	

Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip sla group schedule** **Example:** `Device# show ip sla group schedule`	(Optional) Displays IP SLAs group schedule details.
Step 6	**show ip sla configuration** **Example:** `Device# show ip sla configuration`	(Optional) Displays IP SLAs configuration details.

Configuration Examples for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Example: Dual-Ended Ethernet Delay Operation

The following sample output shows the configuration, including default values, of a receiver MEP on the responder device for a dual-ended Ethernet delay or delay variation operation:

```
Device# show ip sla configuration 501

IP SLAs Infrastructure Engine-III
Entry number: 501
Owner: admin
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: xxx
ReceiveOnly: TRUE
Evc: yyy
Local Mpid: 101
CoS: 3
   Max Delay: 5000
Threshold (milliseconds): 5000
```

```
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

The following sample output shows the configuration, including default values, of the sender MEP for a dual-ended IP SLAs Ethernet delay or delay variation operation:

```
Device# show ip sla configuration 500

IP SLAs Infrastructure Engine-III
Entry number: 500
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: yyy
ReceiveOnly: FALSE
Evc: xxx
Target Mpid: 101
Source Mpid: 100
CoS: 3
   Request size (Padding portion): 64
   Frame Interval: 1000
Threshold (milliseconds): 5000
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
History
  Number of intervals: 22
```

Example: Frame Delay and Frame Delay Variation Measurement Configuration

The following sample output shows the performance monitoring session summary:

```
Device# show ethernet cfm pm session summary

Number of Configured Session : 2
Number of Active Session: 2
Number of Inactive Session: 0
```

The following sample output shows the active performance monitoring session:

```
Device# show ethernet cfm pm session active

Display of Active Session
```

```
------------------------------------------------------------------------------
EPM-ID   SLA-ID    Lvl/Type/ID/Cos/Dir     Src-Mac-address Dst-Mac-address
------------------------------------------------------------------------------
 0     10           3/BD-V/10/2/Down     d0c2.8216.c9d7  d0c2.8216.27a3
 1     11           3/BD-V/10/3/Down     d0c2.8216.c9d7  d0c2.8216.27a3
Total number of Active Session: 2
```

```
Device# show ethernet cfm pm session db 0
```

```
------------------------------------------------------------------------------
      TX Time FWD                   RX Time FWD
      TX Time BWD                   RX Time BWD              Frame Delay
      Sec:nSec                      Sec:nSec                  Sec:nSec
------------------------------------------------------------------------------
Session ID: 0
******************************************************************************
       234:526163572                 245:305791416
       245:306761904                 234:527134653             0:593
******************************************************************************
       235:528900628                 246:308528744
       246:309452848                 235:529825333             0:601
******************************************************************************
       236:528882716                 247:308511128
       247:309450224                 236:529822413             0:601
******************************************************************************
       237:526578788                 248:306207432
       248:307157936                 237:527529885             0:593
******************************************************************************
       238:527052156                 249:306681064
       249:307588016                 238:527959717             0:609
******************************************************************************
       239:526625044                 250:306254200
       250:307091888                 239:527463325             0:593
******************************************************************************
       240:528243204                 251:307872648
       251:308856880                 240:529228021             0:585
```

Example: Sender MEP for a Single-Ended Ethernet Delay Operation

The following sample output shows the configuration, including default values, of the sender MEP for a single-ended IP SLAs Ethernet delay operation:

```
Router# show ip sla configuration 10
```

```
IP SLAs Infrastructure Engine-III
Entry number: 10
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: xxx
Vlan: yyy
Target Mpid: 101
Source Mpid: 100
CoS: 4
   Max Delay: 5000
   Request size (Padding portion): 64
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
```

```
.
.
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

Example: Sender MEP for a Single-Ended Ethernet Frame Loss Operation

The following output shows the configuration, including default values, of the sender MEP in a basic single-ended IP SLAs Ethernet frame loss ratio operation with a start-time of now:

```
Router# show ip sla configuration 11

IP SLAs Infrastructure Engine-III
Entry number: 11
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Loss Operation
Frame Type: LMM
Domain: xxx
Vlan: 12
Target Mpid: 34
Source Mpid: 23
CoS: 4
   Request size (Padding portion): 0
   Frame Interval: 1000
Schedule:
   Operation frequency (seconds): 60  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): ActiveThreshold (milliseconds): 5000
Statistics Parameters
  Aggregation Period: 900
  Frame consecutive: 10
  Availability algorithm: static-window
History
  Number of intervals: 2
```

Additional References for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

Related Documents

Related Topic	Document Title
Cisco IOS Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference
Cisco IOS IP SLAs commands	Cisco IOS IP SLAs Command Reference
Ethernet CFM	"Configuring Ethernet Connectivity Fault Management in a Service Provider Network" module of the *Cisco IOS Carrier Ethernet Configuration Guide*
Network Time Protocol (NTP)	"Configuring NTP" module of the *Cisco IOS Network Management Configuration Guide*
Proactive threshold monitoring for Cisco IOS IP SLAs	"Configuring Proactive Threshold Monitoring of IP SLAs Operations" module of the *Cisco IOS IP SLAs Configuration Guide*

Standards and RFCs

Standard/RFC	Title
ITU-T Y.1731	*OAM functions and mechanisms for Ethernet-based networks*
No specific RFCs are supported by the features in this document.	--

MIBs

MIB	MIBs Link
• CISCO-IPSLA-ETHERNET-MIB • CISCO-RTTMON-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

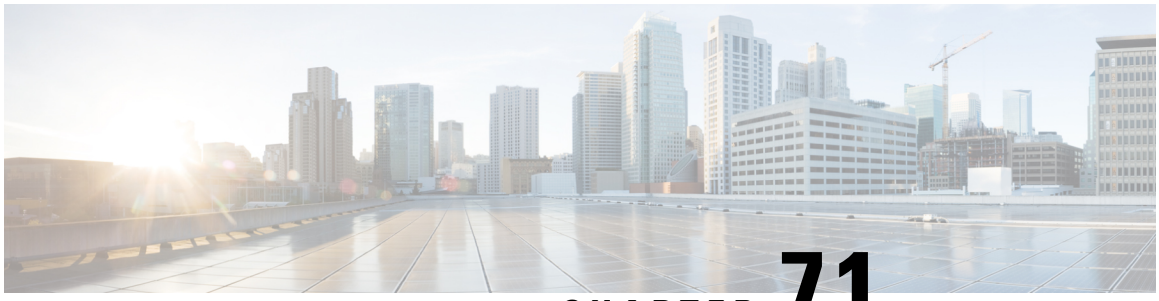
Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) Operations

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 92: Feature Information for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731)

Feature Name	Releases	Feature Information
IP SLA Support for ETH-SLM (Ethernet Synthetic Loss Measurement in Y1731)		Y.1731 Performance Monitoring (PM) provides a standard Ethernet PM function that includes measurement of Ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group.
Y1731 MIB Support through existing IPSLA MIBs		Support was added for reporting threshold events and collecting performance statistics for IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operations using SNMP.



CHAPTER 71

VXLAN-MCLAG Active-Active High Availability Support

The VXLAN-MCLAG Active-Active High Availability Support feature implements dual-home device with pseudo Multichassis Link Aggregation Control Protocol (pMLACP) redundancy mode and layer 2 VxLAN on the Cisco ASR1000 Series Aggregation Services Routers.

Restrictions for VXLAN-MCLAG Active-Active High Availability Support

- The loopback interface configured for this feature cannot be used for another feature.
- The loopback interface of NVE interface must be shut down before configuring pmLACP, VxLAN and routing protocol.
- Bridge domain supports one VXLAN Network Identifier (VNI) Ethernet flow point (EFP) member only.
- Shutting the bridge domain affects status of the NVE interface, not the pseudo mLACP status.

Information About VXLAN-MCLAG Active-Active High Availability Support

Virtual Extensible LAN

Virtual Extensible LAN (VXLAN) is a network virtualization overlay technology that provides Layer 2 connectivity for workloads residing at noncontiguous points in the data center network. VXLAN enables

flexibility by allowing workloads to be placed anywhere, along with the traffic separation required in a multitenant environment. VXLAN is an industry-standard protocol and uses underlay IP networks. It extends Layer 2 segments over a Layer 3 infrastructure to build Layer 2 overlay logical networks. It encapsulates Ethernet frames into IP User Data Protocol (UDP) headers and transports the encapsulated packets through the underlay network to the remote VXLAN tunnel endpoints (VTEPs) using the normal IP routing and forwarding mechanism.

Multichassis Link Aggregation Group

Multichassis Link Aggregation Group (MC-LAG) and Inter-chassis Communication Protocol (ICCP) enable a switch/router to use standard Ethernet Link Aggregation for device dual-homing, with active/standby redundancy. MC-LAG provides a mean to dual home a device (the dual homed device (DHD)) to two different peer devices (the Point of Attachment), allowing to have the benefits of node redundancy. Point of Attachment (PoA) nodes run Inter-chassis Communication Protocol (ICCP) to synchronize state & form a Redundancy Group (RG).

In VXLAN - MCLAG Active-Active High Availability support, both the PoA ports are placed in active/active mode with manual VLAN load balancing. It provides higher bandwidth utilization than Multichassis Link Aggregation Control Protocol (mLACP). It also allows maximum flexibility for the Provider Edge-Customer Edge (PE-CE) inter-operability for dual-homing redundancy and failover recovery. Active and standby PoA nodes are configured on the identical interfaces, that is, the same loopback IP address and interface as VTEP source interface, VLAN and VNI mapping, and so on.

How to Configure VXLAN-MCLAG Active-Active High Availability Support

Configuring Interchassis Redundancy Groups on PoA

To configure interchassis redundancy groups on PoA, perform the steps below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **interchassis group** *group-id*
5. **member ip** *peer ip address*
6. **monitor peer [bfd | track]**
7. **mlacp node-id** *node id*
8. **backbone interface** *backbone if*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**redundancy** **Example:** `Device(config)# redundancy`	Configures the redundancy group.
Step 4	**interchassis group** *group-id* **Example:** `Device(config-red)# interchassis group 2`	Configures interchassis group.
Step 5	**member ip** *peer ip address* **Example:** `Device(config-r-ic)# member ip 172.168.40.24`	Specifies IP address to be assigned to a remote peer dialing in to the interface.
Step 6	**monitor peer [bfd | track]** **Example:** `Device(config-r-ic)# monitor peer bfd`	Specifies the the peer monitoring method.
Step 7	**mlacp node-id** *node id* **Example:** `Device(config-r-ic)# mlacp node-id 2`	Configures mLACP node ID.
Step 8	**backbone interface** *backbone if* **Example:** `Device(config-r-ic)# backbone interface Gi0/0/2`	Configures a backbone interface for the redundancy group.
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Port Channel on PoA

To configure port channel on PoA, perform the steps below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface Port-channel** *port channel number*
4. **negotiation**

5. **lacp fast-switchover**
6. **mlacp interchassis group** *rg id*
7. **mlacp mode active-active**
8. **mlacp load-balance primary vlan** *vlan-id*
9. **mlacp load-balance secondary vlan** *vlan-id*
10. **service instance** *id* **ethernet**
11. **encapsulation dot1q**
12. **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** *port channel number* **Example:** `Device(config-if)# interface Port-channel 2`	Configures the interface for port channel.
Step 4	**negotiation** **Example:** `Device(config-if)# negotiation`	Configures auto negotiation mode.
Step 5	**lacp fast-switchover** **Example:** `Device(config-if)# lacp fast-switchover`	Specifies LACP Port Channel interface.
Step 6	**mlacp interchassis group** *rg id* **Example:** `Device(config-if)# mlacp interchassis group 2`	Configures mLACP peer PoA RG ID.
Step 7	**mlacp mode active-active** **Example:** `Device(config-if)# mlacp mode active-active`	Enables mLACP active-active POA redundancy.
Step 8	**mlacp load-balance primary vlan** *vlan-id* **Example:** `Device(config-if)# mlacp load-balance primary vlan 40`	Configures the list of primary VLANs that will be active and inactive on the given PoA.

	Command or Action	Purpose
Step 9	**mlacp load-balance secondary vlan** *vlan-id* **Example:** `Device(config-if)# mlacp load-balance secondary vlan 20`	Configures the list of secondary VLANs that will be active and inactive on the given PoA.
Step 10	**service instance** *id* **ethernet** **Example:** `Device(config-if-srv)# service instance 20 ethernet`	Configures service instance identifier.
Step 11	**encapsulation dot1q** **Example:** `Device(config-if-srv)# encapsulation dot1q 20`	Configures ethernet frame match criteria.
Step 12	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Vxlan Unicast Core Configuration on POA

To configure Vxlan Unicast Core Configuration on POA, perform the steps below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *id*
4. **member vni** *number*
5. **member Port-channel** *number* **service-instance** *id*
6. **exit**
7. **interface Loopback** *number*
8. **ip address**
9. **exit**
10. **interface nve**
11. **member vni** *number*
12. **ingress-replication** *IPV4 address*
13. **exit**
14. **source-interface Loopback** *id*
15. **no shutdown**
16. **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	**bridge-domain** *id* **Example:** `Device(config)# bridge-domain 20`	Configures the bridge domain ID.
Step 4	**member vni** *number* **Example:** `Device(config-bdomain)# member vni 7777`	Configures member virtual network identifier (VNI).
Step 5	**member Port-channel** *number* **service-instance** *id* **Example:** `Device(config-bdomain)# member Port-channel1 service-instance 20`	Configures port channel and service instance.
Step 6	**exit** **Example:** `Device(config-bdomain)# exit`	Exits bridge domain mode and returns to global configuration mode.
Step 7	**interface Loopback** *number* **Example:** `Device(config-if)# interface Loopback10`	Specifies a loopback interface.
Step 8	**ip address** **Example:** `Device(config-if)# ip address 77.1.1.1 255.255.255.255`	Configures IP address.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 10	**interface nve** **Example:** `Device(config)# interface nve1`	Configures network virtualization endpoint interface.
Step 11	**member vni** *number* **Example:**	Configures VNI information.

	Command or Action	Purpose
	`Device(config-if)# member vni 7777`	
Step 12	**ingress-replication** *IPV4 address* **Example:** `Device(config-if-nve-vni)# ingress-replication 99.1.1.1`	Configures remote Peer IPV4 Address.
Step 13	**exit** **Example:** `Device(config-if-nve-vni)# exit`	Exits network virtualization endpoint interface configuration mode and returns to global configuration mode.
Step 14	**source-interface Loopback** *id* **Example:** `Device(config-if)# source-interface Loopback10`	Configures interface loopback.
Step 15	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts the interface.
Step 16	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Vxlan Multicast Core Configuration on POA

To configure Vxlan Multicast Core Configuration on POA, perform the steps below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *id*
4. **member vni** *number*
5. **member Port-channel** *number* **service-instance** *id*
6. **exit**
7. **interface Loopback** *number*
8. **ip address**
9. **ip pim sparse-dense-mode**
10. **exit**
11. **interface nve**
12. **member vni** *number* **mcast-group** *address*
13. **source-interface Loopback**
14. **no shutdown**
15. **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	**bridge-domain** *id* **Example:** `Device(config)# bridge-domain 20`	Configures the bridge domain ID.
Step 4	**member vni** *number* **Example:** `Device(config-bdomain)# member vni 7777`	Configures member virtual network identifier (VNI).
Step 5	**member Port-channel** *number* **service-instance** *id* **Example:** `Device(config-bdomain)# member Port-channel1 service-instance 20`	Configures port channel and service instance.
Step 6	**exit** **Example:** `Device(config-bdomain)# exit`	Exits bridge domain mode and returns to global configuration mode.
Step 7	**interface Loopback** *number* **Example:** `Device(config-if)# interface Loopback10`	Specifies a loopback interface.
Step 8	**ip address** **Example:** `Device(config-if)# ip address 77.1.1.1 255.255.255.255`	Configures IP address.
Step 9	**ip pim sparse-dense-mode** **Example:** `Device(config-if)# ip pim sparse-dense-mode`	Enables PIM to operate in sparse or dense mode.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**interface nve** **Example:**	Configures network virtualization endpoint interface.

	Command or Action	Purpose
	`Device(config)# interface nve1`	
Step 12	**member vni** *number* **mcast-group** *address* **Example:** `Device(config-if)# member vni 7777 mcast-group 232.1.1.1`	Configures VNI information.
Step 13	**source-interface Loopback** **Example:** `Device(config-if)# source-interface Loopback10`	Configures interface loopback.
Step 14	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts the interface.
Step 15	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Dual-homed Device

To configure dual-homed device, perform the steps below:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface Port-channel** *number*
4. **switchport** *group-id*
5. **switchport trunk encapsulation dot1q**
6. **switchport trunk allowed vlan 20-50**
7. **switchport mode trunk**
8. **exit**
9. **interface GigabitEthernet3/1**
10. **switchport**
11. **switchport trunk encapsulation dot1q**
12. **switchport trunk allowed vlan 20-50**
13. **switchport mode trunk**
14. **channel-group** *number mode*
15. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface Port-channel** *number* **Example:** `Device(config)# interface Port-channel1`	Configures ethernet channel of interfaces.
Step 4	**switchport** *group-id* **Example:** `Device(config-if)# switchport`	Sets the interface as an Ethernet interface.
Step 5	**switchport trunk encapsulation dot1q** **Example:** `Device(config-r-ic)# switchport trunk encapsulation dot1q`	Defines the encapsulation format as IEEE 802.1Q (dot1q) for the specified interface.
Step 6	**switchport trunk allowed vlan 20-50** **Example:** `Device(config-r-ic)# switchport trunk allowed vlan 20-50`	Specifies that only certain VLANs are allowed on the specified trunk.
Step 7	**switchport mode trunk** **Example:** `Device(config-r-ic)# switchport mode trunk`	Sets the interface as an Ethernet trunk port.
Step 8	**exit** **Example:** `Device(config-r-ic)# exit`	Exits interface mode and returns to global configuration mode
Step 9	**interface GigabitEthernet3/1** **Example:** `Device(config-if)# interface GigabitEthernet3/1`	Enters the interface configuration mode on the Gigabit Ethernet interface.
Step 10	**switchport** **Example:** `Device(config-if)# switchport`	Configures the interface port.
Step 11	**switchport trunk encapsulation dot1q** **Example:** `Device(config-if)# switchport trunk encapsulation dot1q`	Defines the encapsulation format as IEEE 802.1Q (dot1q) for the specified interface.

	Command or Action	Purpose
Step 12	**switchport trunk allowed vlan 20-50** **Example:** `Device(config-if)# switchport trunk allowed vlan 20-50`	Specifies that only certain VLANs are allowed on the specified trunk.
Step 13	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Sets the interface as an Ethernet trunk port.
Step 14	**channel-group** *number mode* **Example:** `Device(config-if)# channel-group 1 mode active`	Configures the port in a channel group and sets the mode.
Step 15	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying VXLAN-MCLAG Active-Active High Availability Support

To verify, perform the steps below.

SUMMARY STEPS

1. **show lacp internal**
2. **show nve interface nve1**
3. **show nve peers**
4. **show platform software ethernet fp ac bridge-domain binding**
5. **show bridge-domain 20**
6. **show lacp multi-chassis load-balance port-channel**
7. **show nve vni 11111 detail**
8. **show lacp multi load group**

DETAILED STEPS

Step 1 **show lacp internal**

Example:

```
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
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi0/0/0   SA      bndl      32768         0x1       0x1     0x1         0x3D

Channel group 2
```

```
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi0/0/1   SA      susp      32768         0x2       0x2     0x2         0x7D
```

Step 2 **show nve interface nve1**

Example:

```
Interface: nve1, State: Admin Up, Oper Up Encapsulation: Vxlan
source-interface: Loopback10 (primary:77.1.1.1 vrf:0)
```

Step 3 **show nve peers**

Example:

```
Interface  Peer-IP          VNI        Peer state
   nve1    99.1.1.1         7777
```

Step 4 **show platform software ethernet fp ac bridge-domain binding**

Example:

```
Forwarding Manager Bridge Domain Bindings

BD    Interface                      EFP DPIDB  SHG   STP  AOM id
------------------------------------------------------------------------------
20    Port-channel1.EFP20            16908305   None FRWD 182, (created)
20    nve1.VNI7777                   16908307   None FRWD 268, (created)
40    Port-channel1.EFP40            16908306   None BLCK 258, (created)
40    nve2.VNI8888                   16908308   None FRWD 285, (created)
```

Step 5 **show bridge-domain 20**

Example:

```
FBridge-domain 20 (2 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    Port-channel1 service instance 20
    vni 7777
   AED MAC address    Policy  Tag       Age  Pseudoport
   0   0000.6177.0003 forward dynamic   300  nve1.VNI7777, VxLAN
                                           src: 77.1.1.1 dst: 99.1.1.1
   0   0000.6177.0009 forward dynamic   300  nve1.VNI7777, VxLAN
                                           src: 77.1.1.1 dst: 99.1.1.1
   0   0000.6177.0000 forward dynamic   300  nve1.VNI7777, VxLAN
                                           src: 77.1.1.1 dst: 99.1.1.1
   0   0000.1577.0009 forward dynamic   300  Port-channel1.EFP20
```

Step 6 **show lacp multi-chassis load-balance port-channel**

Example:

```
Interface Port-Channel 1
        Local Configuration:
                P-mLACP Enabled:      Yes
                Redundancy Group:     1
                Revertive Mode:       Revertive
                Primary VLANs:        20
                Secondary VLANs:      40
        Local Interface State:
                Interface ID: 1
                Port State:           Up
                Primary VLAN State:   Active
                Secondary VLAN State: Standby
        Peer Interface State:
```

```
                Interface ID: 1
                Primary VLAN State:   Active
                Secondary VLAN State: Standby
```

Step 7 **show nve vni 11111 detail**

Example:

```
IInterface  VNI        Multicast-group  VNI state
nve1       11111      N/A              Up
VNI Detailed statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
1682112875 107655224000 1681321674 107604587136
```

Step 8 **show lacp multi load group**

Example:

```
Interchassis Redundancy Group 1

                RG State:       Synchronized
                ICCP Version:   0
        Backbone Uplink Status: Connected
        Local Configuration:
                Node-id:        0

        Peer Information:
                State:          Up
                Node-id:        1
                ICCP Version:   0

States:      Active     - ACT           Standby    - SBY
             Down       - DN            AdminDown  - ADN
             Unknown    - UN            Reverting  - REV

P-mLACP Interfaces
Interface    Port State     Local VLAN State      Peer VLAN State
   ID          Local       Primary/Secondary     Primary/Secondary
   1             UP             ACT/SBY               ACT/SBY
```

Configuration Examples for VXLAN-MCLAG Active-Active High Availability Support

Example: Configuring VXLAN HA on Multicast Mode

The following example shows how to configure the VXLAN-MCLAG Active-Active High Availability Support feature on a multicast mode with two points of attachments (POA) connected to branch devices. The following is the configuration on the first POA—POA1.

```
ip multicast-routing distributed
ip pim bidir-enable
ip pim rp-address 4.4.4.4 bidir

redundancy
 mode sso
```

```
 interchassis group 1
  monitor peer bfd
  member ip 9.9.9.9
  backbone interface GigabitEthernet0/1/0
  mlacp system-priority 200
  mlacp node-id 0

bridge-domain 20
 member vni 7777
 member Port-channel1 service-instance 20
!

bridge-domain 40
 member vni 8888
 member Port-channel1 service-instance 40
!
interface Loopback10
 ip address 77.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback11
 ip address 88.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface Port-channel1
 no ip address
 negotiation auto
 lacp fast-switchover
 mlacp interchassis group 1
 mlacp mode active-active
 mlacp load-balance primary vlan 40
 mlacp load-balance secondary vlan 20
 service instance 20 ethernet
  encapsulation dot1q 20
 !
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
interface nve1
 no ip address
 member vni 7777 mcast-group 225.1.1.1
 source-interface Loopback10
!
interface nve2
 no ip address
 member vni 8888 mcast-group 226.1.1.1
 source-interface Loopback11
!

interface GigabitEthernet0/1/0
 ip address 192.168.20.1 255.255.255.0
 ip pim sparse-dense-mode
 negotiation auto
!

router ospf 10
 router-id 3.3.3.3
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the second POA—POA2.

```
ip multicast-routing distributed
ip pim bidir-enable
```

```
ip pim rp-address 4.4.4.4 bidir

redundancy
 mode sso
 interchassis group 1
  monitor peer bfd
  member ip 3.3.3.3
  backbone interface GigabitEthernet0/0/1
  mlacp system-priority 200
  mlacp node-id 1

bridge-domain 20
 member vni 7777
 member Port-channel1 service-instance 20
!

bridge-domain 40
 member vni 8888
 member Port-channel1 service-instance 40
!

interface Loopback10
 ip address 77.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback11
 ip address 88.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface Port-channel1
 no ip address
 negotiation auto
 no keepalive
 lacp fast-switchover
 mlacp interchassis group 1
 mlacp mode active-active
 mlacp load-balance primary vlan 20
 mlacp load-balance secondary vlan 40
 service instance 20 ethernet
  encapsulation dot1q 20
 !
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
interface nve1
 no ip address
 member vni 7777 mcast-group 225.1.1.1
 source-interface Loopback10
!
interface nve2
 no ip address
 member vni 8888 mcast-group 226.1.1.1
 source-interface Loopback11
!

interface GigabitEthernet0/1/0
 ip address 192.168.20.1 255.255.255.0
 ip pim sparse-dense-mode
 negotiation auto
!

interface GigabitEthernet0/0/1
 ip address 192.168.4.1 255.255.255.0
```

```
 ip pim sparse-dense-mode
 negotiation auto
end

router ospf 10
 router-id 9.9.9.9
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the first branch—Branch1.

```
ip multicast-routing distributed
ip pim bidir-enable
ip pim rp-address 4.4.4.4 bidir
!
bridge-domain 20
 member vni 7777
 member GigabitEthernet0/0/0 service-instance 20
!
interface Loopback10
 ip address 99.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface nve1
 no ip address
 member vni 7777 mcast-group 225.1.1.1
 source-interface Loopback10
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
 service instance 20 ethernet
  encapsulation dot1q 20
 !
!
interface GigabitEthernet0/0/0
 ip address 192.168.3.1 255.255.255.0
 ip pim sparse-dense-mode
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the second branch—Branch2.

```
ip multicast-routing distributed
ip pim bidir-enable
ip pim rp-address 4.4.4.4 bidir
!
bridge-domain 40
 member vni 8888
 member GigabitEthernet0/0/0 service-instance 40
!
interface Loopback11
 ip address 100.1.1.1 255.255.255.255
 ip pim sparse-dense-mode
!
interface nve1
 no ip address
 member vni 8888 mcast-group 226.1.1.1
 source-interface Loopback11
!
interface GigabitEthernet0/0/0
no ip address
 negotiation auto
```

```
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
interface GigabitEthernet0/0/1
 ip address 192.168.21.1 255.255.255.0
 ip pim sparse-dense-mode
negotiation auto
!
router ospf 10
network 0.0.0.0 255.255.255.255 area 10
!
```

Example: Configuring VXLAN HA on Unicast Mode

The following example shows how to configure the VXLAN-MCLAG Active-Active High Availability Support feature on an unicast mode with two points of attachments (POA) connected to branch devices. The following is the configuration on the first POA—POA1.

```
redundancy
 mode sso
 interchassis group 1
  monitor peer bfd
  member ip 9.9.9.9
  backbone interface GigabitEthernet0/1/0
  mlacp system-priority 200
  mlacp node-id 0

bridge-domain 20
 member vni 7777
 member Port-channel1 service-instance 20
!

bridge-domain 40
 member vni 8888
 member Port-channel1 service-instance 40
!
interface Loopback10
 ip address 77.1.1.1 255.255.255.255
!
interface Loopback11
 ip address 88.1.1.1 255.255.255.255
!
interface Port-channel1
 no ip address
 negotiation auto
 lacp fast-switchover
 mlacp interchassis group 1
 mlacp mode active-active
 mlacp load-balance primary vlan 40
 mlacp load-balance secondary vlan 20
 service instance 20 ethernet
  encapsulation dot1q 20
 !
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
interface nve1
 no ip address
 member vni 7777
```

```
  ingress-replication 99.1.1.1
 !
 source-interface Loopback10
!
interface nve2
 no ip address
 member vni 8888
  ingress-replication 100.1.1.1
 !
 source-interface Loopback11
!

router ospf 10
 router-id 3.3.3.3
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the second POA—POA2.

```
redundancy
 mode sso
 interchassis group 1
  monitor peer bfd
  member ip 3.3.3.3
  backbone interface GigabitEthernet0/0/1
  mlacp system-priority 200
  mlacp node-id 1

bridge-domain 20
 member vni 7777
 member Port-channel1 service-instance 20
!

bridge-domain 40
 member vni 8888
 member Port-channel1 service-instance 40
!

interface Loopback10
 ip address 77.1.1.1 255.255.255.255
!
interface Loopback11
 ip address 88.1.1.1 255.255.255.255
!
interface Port-channel1
 no ip address
 negotiation auto
 no keepalive
 lacp fast-switchover
 mlacp interchassis group 1
 mlacp mode active-active
 mlacp load-balance primary vlan 20
 mlacp load-balance secondary vlan 40
 service instance 20 ethernet
  encapsulation dot1q 20
 !
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
interface nve1
 no ip address
 member vni 7777
  ingress-replication 99.1.1.1
 !
```

```
 source-interface Loopback10
!
interface nve2
 no ip address
 member vni 8888
  ingress-replication 100.1.1.1
 !
 source-interface Loopback11
!

router ospf 10
 router-id 9.9.9.9
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the first branch—Branch1.

```
bridge-domain 20
 member vni 7777
 member GigabitEthernet0/0/0 service-instance 20
!
interface Loopback10
 ip address 99.1.1.1 255.255.255.255
!
interface nve1
 no ip address
 member vni 7777
     ingress-replication 77.1.1.1
 source-interface Loopback10
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
 service instance 20 ethernet
  encapsulation dot1q 20
 !
!
router ospf 10
 network 0.0.0.0 255.255.255.255 area 10
!
```

The following is the configuration on the second branch—Branch2.

```
bridge-domain 40
 member vni 8888
 member GigabitEthernet0/0/0 service-instance 40
!
interface Loopback11
 ip address 100.1.1.1 255.255.255.255
!
interface nve1
 no ip address
 member vni 8888
     ingress-replication 88.1.1.1
 source-interface Loopback11
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
 service instance 40 ethernet
  encapsulation dot1q 40
 !
!
router ospf 10
```

```
 network 0.0.0.0 255.255.255.255 area 10
!
```

Additional References for VXLAN-MCLAG Active-Active High Availability Support

Related Documents

Related Topic	Document Title
Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

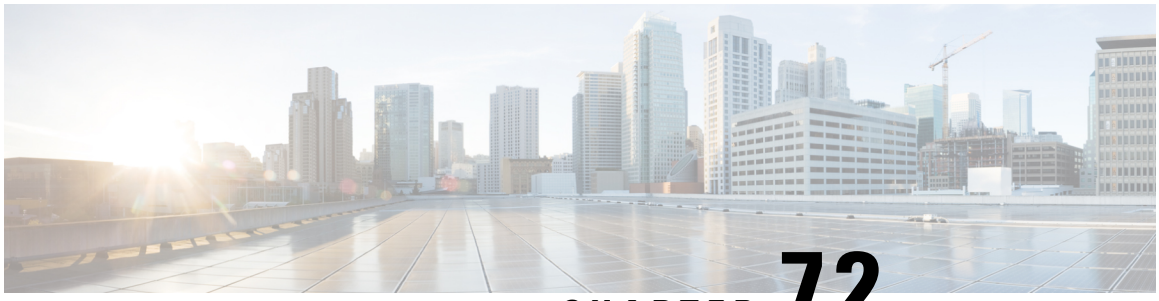
Feature Information for VXLAN-MCLAG Active-Active High Availability Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 93: Feature Information for VXLAN-MCLAG Active-Active High Availability Support

Feature Name	Releases	Feature Information
VXLAN-MCLAG Active-Active High Availability Support	Cisco IOS XE 3.16S	The VXLAN-MCLAG Active-Active High Availability Support feature implements dual-home device with pseudo Multichassis Link Aggregation Control Protocol (pMLACP) redundancy mode and layer 2 VXLAN on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced by this feature: **show lacp internal, show nve interface nve1, show nve peersshow platform software ethernet fp ac bridge-domain binding, show bridge-domain 20, show lacp multi-chassis load-balance port-channel, show nve vni 11111 detail, show lacp multi load group**



CHAPTER 72

VxLAN Support

This module contains information about VxLAN (Virtual eXtensible Local Area Network) Layer 2 gateway feature support on the Cisco ASR 1000 Series Routers. VxLAN is a technology that provides a Layer 2 overlay network, allowing for network isolation. The standard 802.1q VLAN implementation limits the number of tags to 4096. However, cloud service providers may want to operate more than 4096 virtual networks. VxLAN uses a 24-bit network ID, which allows for a much larger number of individual i networks to be operated.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for VxLAN Support

The following are the prerequisites to configuring the Cisco ASR 1000 Routers as a VxLAN Layer 2 gateway:

1. Configure the loopback interface.
2. Configure the IP unicast reachability to remote VTEP's.
3. Configure Bidirectional Protocol Independent Multicast (PIM) or Protocol Independent Multicast-Sparse Mode (PIM-SM).

For more information, see the IP Multicast: PIM Configuration Guide, Cisco IOS XE Release 3S .

Information About VxLAN Support

This feature enables the Cisco ASR 1000 Series Routers to act as a Layer 2 VxLAN gateway to provide support to bridge traffic across VxLAN segments in a hypervisor and on VLANs on physical servers. The operation of a VxLAN Layer 2 gateway is based on the data plane MAC address learning and flooding of multidestination traffic (such as unknown unicast, multicast, or broadcast frames) using IP multicast.

Acting as a VxLAN Layer 2 gateway, the Cisco ASR 1000 Routers can send and receive packets on multiple VxLAN networks, and provide connectivity between the hosts in a VLAN network and the virtual machines operating on a VxLAN network.

A VXLAN supports different modes for flood traffic:

- Multicast Mode—A VXLAN uses an IP multicast network to send broadcast, multicast, and unknown unicast flood frames. Each multicast mode VXLAN has an assigned multicast group IP address. When a new VM joins a host in a multicast mode VXLAN, the Virtual Tunnel Endpoint (VTEP) joins the assigned multicast group IP address by sending IGMP join messages. Flood traffic, broadcast, multicast and unknown unicast from the VM is encapsulated and is sent using the assigned multicast group IP address as the destination IP address. Packets sent to known unicast MAC addresses are encapsulated and sent directly to the destination server Virtual Tunnel Endpoint (VTEP) IP addresses.
- Unicast-Only Mode—A VXLAN uses each VEM's single unicast IP address as the destination IP address to send broadcast, multicast, and unknown unicast flood frames of the designated VTEP on each VEM that has at least one VM in the corresponding VXLAN. When a new VM joins the host in a unicast-mode VXLAN, a designated VTEP is selected for receiving flood traffic on that host. This designated VTEP is communicated to all other hosts through the Virtual Supervisor Module (VSM). Flood traffic (broadcast, multicast, and unknown unicast) is replicated on each VEM's designated VTEP in that VXLAN by encapsulating it with a VXLAN header. Packets are sent only to VEMs with a VM in that VXLAN. Packets that have a unicast MAC address are encapsulated and sent directly to the destination server's VTEP IP address.
- MAC Distribution Mode (supported only in unicast mode)—In this mode, unknown unicast flooding in the network is eliminated. The VSM learns all the MAC addresses from the VEMs in all the VXLANs and distributes those MAC addresses with VTEP IP mappings to other VEMs. Therefore, no unknown unicast MAC address exists in the network when the VMs on the VEMs are communicating and controlled by the same VSM.

The VxLAN Layer 2 gateway performs the following functions:

- Provides support to bridge traffic between a host in a VLAN domain and VMs behind a virtual switch (vSwitch) in a VxLAN domain. The VLAN and the virtual network identifier (VNI) on the VxLAN should be configured as member ports in the same bridge domain.
- Implements the Virtual Tunnel Endpoint (VTEP) function, which encapsulates the Layer 2 packet on the IP/UDP tunnel with the VxLAN header (VNI) information before sending it to a multicast group or particular virtual switch on the VxLAN domain.
- The VTEP function removes the VxLAN header, identifies the bridge domain under which the VNI is configured and then bridges the inner L2 packet to the VLAN side. The bridge function also learns the remote MAC address (the VM's MAC address behind the virtual switch).
- The Layer 2 gateway carries the inner payload of non-IP (Layer 2 traffic), IPv4, and IPv6 traffic over the VxLAN VNI member.

Limitations of VxLAN Support

1. Platforms that support a new scale number (8192 or 16000) require an 8G RP memory. Scale number for RP memory that is less than 8G is unchanged.
2. Scale number on platform RP+ESP5 and ASR1002F is unchanged.
3. VxLAN is not supported on ISR4000 series platforms before Cisco IOS XE Everest 16.5.1.
4. The maximum NVE interface number is unchanged on all platforms.
5. The NVE source is supported for lookback interface before Cisco IOS XE Denali 16.3. After Cisco IOS XE Denali 16.3, it can support physical interfaces as well.
6. The scale enhancement is applicable only for the VxLAN layer 2 and layer 3 gateway feature. Other bridge-domain related features are not impacted.
7. RP switchover for VxLAN is not supported on these platforms before Cisco IOS XE Denali 16.3.
8. Only one VNI ID on every bridge-domain is supported.

New Scale Number after Enhancements

The following table lists new VxLAN scale numbers on different platforms after enhancements. All platforms that support a new scale number (8192 or 16000) require an 8G RP memory.

Platform	MAX BD per system	MAX BDI interface per system	MAX VNI per system
RP+ESP200	16000	16000	16000
RP+ESP100	16000	16000	16000
RP+ESP40	16000	16000	16000
RP+ESP20	16000	16000	16000
RP+ESP10	16000	16000	16000
ASR1002-X	16000	16000	16000
ASR1001-X	16000	16000	16000
ASR 1001	8192	8192	8192
CSR1000v	8192	8192	8192

Configuring VxLAN Layer 2 Gateway with Multicast

Configuring the VxLAN UDP Destination Port (Optional)

The default VxLAN UDP destination is 4789. If you want to change the VxLAN UDP destination port value, you must change it before configuring the network virtualization endpoint (NVE) interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vxlan udp port** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `router# configure terminal`	Enters global configuration mode.
Step 3	**vxlan udp port** *number* **Example:** `Router(config)# vxlan udp port 1000`	Configures the VxLAN UDP destination port number. The default value is 4789.

Creating the Network Virtualization Endpoint (NVE) Interface

You create the network virtualization endpoint (NVE) interface and then assign member virtual network identifiers (VNIs) to it. The mapping between the VNI range and the multicast group range is either one-to-one or many-to-one.

SUMMARY STEPS

1. **interface nve** *number*
2. **source-interface loopback** *number*
3. **member vni** {*range* | *startnumber-endnumber*} **multicast-group** *startip-address endip-address*
4. **member vni** *range*
5. **ingress-replication** *Unicast IP Addresses*
6. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface nve** *number* **Example:** `Router(config)# interface nve 1`	Creates a network virtualization endpoint (NVE) interface and enters NVE interface configuration mode.
Step 2	**source-interface loopback** *number* **Example:** `Router(config-if)# source-interface loopback 0`	Assigns the previously-created loopback interface to the NVE interface.
Step 3	**member vni** {*range* | *startnumber-endnumber*} **multicast-group** *startip-address endip-address* **Example:** `Router(config-if)# member vni 7115 multicast-group 225.1.1.1`	Creates a VNI member or a range of VNI members. Repeat this step for each VNI to be added to the NVE interface. The valid values for the VNI number are from 4096 to 16777215.
Step 4	**member vni** *range* **Example:** `Router(config-if)# member vni 7115`	Creates a VNI member or a range of VNI members. Repeat this step for each VNI to be added to the NVE interface. The valid values for the VNI number are from 4096 to 16777215.

Step 5	**ingress-replication** *Unicast IP Addresses*
	Example:
	`Router(config-if-nve-vni)# ingress-replication 225.1.1.1`
	`ingress-replication 225.1.1.2`
		Sets up ingress-replication unicast addresses which enables the headend replication functionality.

Step 6	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the NVE interface.

Creating the Access Ethernet Flow Point (EFP)

After the member VNI is created, you must create the access Ethernet Flow Point (EFP) for the VLAN interface.

SUMMARY STEPS

1. **interface GigabitEthernet** *number*
2. service instance *id* ethernet
3. encapsulation dot1q *vlan-ID*

4. rewrite ingress tag pop 1 symmetric

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface GigabitEthernet** *number* **Example:** `Router(config)# interface GigabitEthernet1`	Enters interface configuration mode.
Step 2	service instance *id* ethernet **Example:** `Router(config-if)# service instance 20 ethernet`	Configures an Ethernet service instance on the overlay interface being configured and enters service instance configuration mode. • The service instance identifier range is from 1 to 8000.
Step 3	encapsulation dot1q *vlan-ID* **Example:** `Router(config-if-srv)# encapsulation dot1q 100`	Defines the VLAN encapsulation format as IEEE 802.1Q and specifies the VLAN identifier.
Step 4	rewrite ingress tag pop 1 symmetric **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Removes the VLAN tag in the Layer 2 traffic before switching to the outgoing VxLAN interface. **Note** This command is required to remove the VLAN tag before sending the VLAN traffic to VxLAN and adding the VLAN tag in the reverse direction.

Mapping the VLAN to the Bridge Domain

You must map the VLAN created in the previous procedure to the bridge domain.

SUMMARY STEPS

1. **bridge-domain** *bridge-id*
2. **member** *interface* **service-instance** *id*
3. **member vni** *vni-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**bridge-domain** *bridge-id* **Example:** `Router(config)# bridge-domain 10`	Creates a bridge domain and enters bridge domain configuration mode. The valid range for bridge-id is 1-4096.
Step 2	**member** *interface* **service-instance** *id* **Example:**	Binds the bridge domain to the service instance.

	Command or Action	Purpose
	`Router(config-bdomain)# member gigabitEthernet 1 service-instance 1`	
Step 3	**member vni** *vni-id* **Example:** `Router(config-bdomain)# member vni 1010`	Maps the VNI to the bridge domain.

What to do next

The following example displays the NVE VNIs configured on the router:

```
Router# show nve vni

Interface  VNI          mcast       VNI state
nve1       5000         230.1.1.1       UP        L2DP 2 N/A
```

The following example displays the NVE VNIs assigned to NVE interface 1:

```
Router(config)# show nve vni interface nve1
Interface  VNI          mcast       VNI state
nve1       5000         230.1.1.1       UP        L2DP 2 N/A
```

The following example shows the status of NVE interface 1:

```
Router(config)# show nve interface nve1
Interface: nve1, State: Admin Up, Oper Up Encapsulation: Vxlan
source-interface: Loopback0 (primary:11.11.11.11 vrf:0)
```

The following example shows a detailed display for NVE interface 1:

```
Router(config)# show nve interface nve1 detail
Interface: nve1, State: Admin Up, Oper Up Encapsulation: Vxlan
source-interface: Loopback0 (primary:11.11.11.11 vrf:0)
Pkts In   Bytes In   Pkts Out  Bytes Out
0          0          0          0
```

The following example shows the NVE peers configured on the router:

```
Router(config)# show nve peers
Interface Peer-IP         VNI      Up Time
nve1        230.1.1.1     5000       UP        L2DP 2 N/A
nve2       1.1.1.3        2030      20h
```

The following example shows the bridge domain configuration with the entry in bold displaying the VM's MAC address that was learned on the VxLAN VNI:

```
Router# show bridge-domain 1000
Bridge-domain 1000 (3 ports in all)
State: UP                    Mac learning: Enabled
Aging-Timer: 300 second(s)
    GigabitEthernet1 service instance 1000
    GigabitEthernet3 service instance 1000
    vni 7639335
   MAC address    Policy  Tag      Age  Pseudoport
```

```
   0050.56A4.ECD2 forward dynamic  297  nve1.VNI7639335 VxLAN
src:10.0.0.1  dst:10.0.0.2
   0050.56A4.257A forward dynamic  297  GigabitEthernet3.EFP1000
```

Configuring VxLAN Layer 2 Gateway with Unicast

The following example shows VxLAN with unicast ingress-replication which is a point-to-point (unicast) configuration.

```
interface Loopback0
ip address 11.11.11.11 255.255.255.255
!
interface nve1
no ip address
member vni 5001
  ingress-replication 22.22.22.22  < Remote L2 GW loopback ip>
!
source-interface Loopback0
!
bridge-domain 1
member vni 5001
member GigabitEthernet0/2/0 service-instance 1
interface GigabitEthernet0/2/0
service instance 1 ethernet
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
```

Feature Information for VxLAN Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

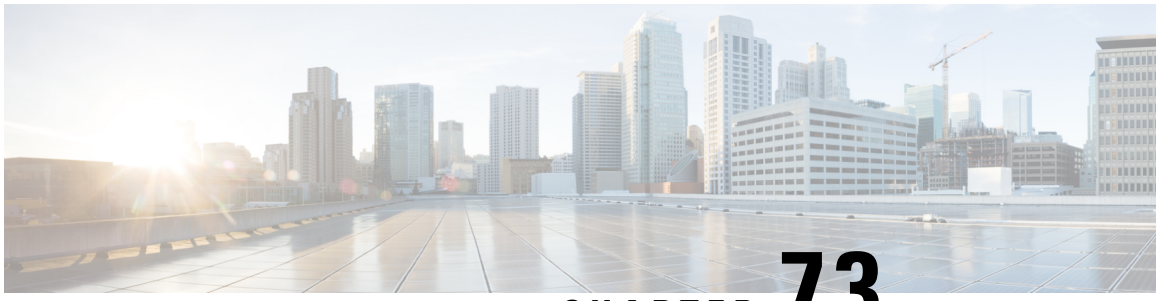
Table 94: Feature Information for VxLAN Support

Feature Name	Releases	Feature Configuration Information
VxLAN Support	Cisco IOS XE Release 3.13.1S Cisco IOS XE Fuji 16.9	This feature was introduced on the Cisco ASR 1000 Series Routers. This feature was introduced on the following: • Cisco ISR 1000 Series Integrated Services Routers. • Cisco ISR 4000 Series Integrated Services Routers.
Protocol Independent Multicast-Sparse Mode (PIM-SM) Support	Cisco IOS XE Release 3.17S	This feature was introduced on the Cisco ASR 1000 Series Routers. No commands were introduced or modified for this feature.

Feature Name	Releases	Feature Configuration Information
Support for multiple ingress replication peers	Cisco IOS XE Everest 16.5.1b	The VXLAN feature was modified to support multiple ingress replication peers on the Cisco ASR 1000 Series Routers. The **ingress-replication** command was modified to support multiple replication peers for every VNI up to 32 nodes.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 73

VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

VxLAN (Virtual eXtensible Local Area Network) GPE (Generic Protocol Extension) is intended to extend the existing VxLAN protocol to provide protocol typing, OAM, and versioning capabilities.

Restrictions for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

- VxLAN GPE tunnel and VxLAN dummy-L2 tunnel do not support IS-IS.
- Layer2 traffic is not supported.
- IPv6 for underlay encapsulation is not supported.

Information About VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Overview

Virtual eXtensible Local Area Network (VxLAN) defines an encapsulation format that encapsulates Ethernet frames in an outer UDP/IP transport. As data centers evolve, the need to carry other protocols encapsulated in an IP packet is required, and the need to provide increased visibility and diagnostic capabilities within the overlay. The VxLAN header does not specify the protocol being encapsulated and therefore is currently limited to encapsulating only Ethernet frame payload, nor does it provide the ability to define Operations, Administration, and Maintenance (OAM) protocols. In addition, new transports need not use transport layer port numbers to identify tunnel payload, rather it encourages encapsulations to use their own identifiers for this purpose. VxLAN GPE (Generic Protocol Extension) is intended to extend the existing VxLAN protocol to provide protocol typing, OAM and versioning capabilities.

The following are the main features of VxLAN GPE Tunnel:

- Encapsulates layer-3 packets directly into a VxLAN tunnel without any layer-2 bridge-domain requirements or dependencies.
- Provides an equal-cost multi-path (ECMP) entropy benefits on the underlay (core) network by calculating the outer-source UDP port based on the inner IP protocol, source or destination IP addresses and L4 port numbers (5-tuple).
- Leverages VxLAN-GPE draft-IETF, which provides direct upper layer protocols options such as, IPv4, IPv6, Ethernet (MAC), Network-Service-Header (NSH) without a layer-2 header.
- Overlay encapsulation is supported for both IPv4 and IPv6, whereas underlay encapsulation is supported only for IPv4.
- 8K Tunnel interfaces with VxLAN GPE or VxLAN dummy-L2 mode are supported.
- 3-tuple hash is enabled to generate UDP source port for both VxLAN GPE and VxLAN Dummy-L2 tunnels for all the packets.
- UDP source port hash uses 3 tuples for fragments, and 5 tuples for non-fragments.

Feature Information for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 95: Feature Information for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Feature Name	Releases	Feature Information
VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel	Cisco IOS XE Denali 16.3.1	The following commands were introduced by this feature: **vxlan gpe-tunnel-udp-port xxx**.
Manually configure the source port range for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel	Cisco IOS XE Everest 16.5.1b	The following commands were introduced by this feature: • **vxlan source-port-range udp** • **vxlan source-port-range gpe-tunnel-udp** • **vxlan source-port-range dummy-l2-tunnel-udp**
Microsoft - VxLAN GPE Tunnel IPv6 Support VxLAN 8K GPE Tunnel Support	Cisco IOS XE Fuji 16.7.1	Overlay encapsulation is supported for both IPv4 and IPv6, whereas underlay encapsulation is supported only for IPv4. 8K Tunnel interfaces with VxLAN GPE or VxLAN dummy-L2 mode are supported.

Feature Name	Releases	Feature Information
VXLAN Fragment UDP Source Port	Cisco IOS XE 16.8.1	Global tunnel CLIs are added to enable 3-tuple hash to generate UDP source port for both VxLAN-GPE and VxLAN Dummy-L2 tunnels. Support both global and under interface tunnel.
IPv6 VxLAN GPE Tunnel and IPv6 VxLAN Dummy-L2 Tunnel	Cisco IOS XE Gibraltar 16.12.1	VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel support IPv6 tunnel mode.

How to Configure VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Configuring VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

1. Configure Vxlan GPE Tunnel on VTEP1.

```
interface Tunnel1
  ip address 192.168.1.1 255.255.255.0
  tunnel source GigabitEthernet2
  tunnel mode vxlan-gpe ipv4
  tunnel destination 20.1.1.17
  tunnel vxlan vni 123456
```

2. Configure Vxlan GPE Tunnel on VTEP2.

```
interface Tunnel1
  ip address 192.168.1.2 255.255.255.0
  tunnel source GigabitEthernet2
  tunnel mode vxlan-gpe ipv4
  tunnel destination 20.1.1.16
  tunnel vxlan vni 123456
```

3. Configure Vxlan Dummy-L2 Tunnel on VTEP1.

```
interface Tunnel0
  ip address 192.168.2.3 255.255.255.0
  tunnel source GigabitEthernet2
  tunnel mode vxlan ipv4 default-mac
  tunnel destination 20.1.1.17
  tunnel vxlan vni 123456
```

4. Configure Vxlan Dummy-L2 Tunnel on VTEP2.

```
interface Tunnel1
  ip address 192.168.2.1 255.255.255.0
  tunnel source GigabitEthernet2
  tunnel mode vxlan ipv4 default-mac
  tunnel destination 20.1.1.16
  tunnel vxlan vni 123456
```

5. (Optional) Change UDP dst port for Vxlan Dummy-L2 Tunnel. Default UDP port of Dummy-L2 Tunnel is 4789.

```
(config)#vxlan dummy-l2-tunnel-udp-port 4789
```

6. (Optional) Change UDP dst port for Vxlan GPE Tunnel. Default UDP port of GPE Tunnel is 4790.

```
(config)#vxlan gpe-tunnel-udp-port 4790
```

Verifying VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

```
##show platform software vxlan fp active udp-port
VXLAN UDP Port: 6000
VXLAN GPE Tunnel UDP Port: 4000
VXLAN Dummy L2 Tunnel UDP Port: 6000
VXLAN UDP Source Port Range: 1025 - 65535
VXLAN GPE Tunnel UDP Source Port Range: 1025 - 65535
VXLAN Dummy L2 Tunnel UDP Source Port Range: 1025 – 65535
VXLAN GPE Tunnel UDP Source Port Hash: 3 tuples
VXLAN  Dummy L2 Tunnel UDP Source Port Hash: 3 tuples
```

Perform the following steps to add new tunnel mode:

```
#interface tunnel0
     tunnel mode vxlan ipv4 default-mac | xxxx.xxxx.xxxx xxxx.xxxx.xxxx


#interface tunnel1
    tunnel mode vxlan-gpe ipv4
```

Perform the following steps to add VxLAN VNI in tunnel:

```
#interface tunnel0
tunnel vxlan vni xxxx
```

Perform the following steps to add VxLAN source port hash in tunnel:

```
#interface tunnel0
vxlan source-port-hash 3-tuple
vxlan source-port-hash 3-tuple-for-fragments
```

Configuration Examples for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Example: VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Example: VxLAN GPE Tunnel

```
#interface Tunnel0
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2001::1/64
 tunnel source GigabitEthernet2
 tunnel mode vxlan ipv4 default-mac
 tunnel destination 20.1.1.16
 tunnel vxlan vni 123456
```

```
#interface Tunnel1
 ip address 192.168.1.2 255.255.255.0
 ipv6 address 2002::2/64
 tunnel source GigabitEthernet2
 tunnel mode vxlan-gpe ipv4
 tunnel destination 20.1.1.16
 tunnel vxlan vni 123456


#sh pl soft vxlan f0 udp-port
VXLAN UDP Port: 4789
VXLAN GPE Tunnel UDP Port: 4790
VXLAN Dummy L2 Tunnel UDP Port: 4789
VXLAN UDP Source Port Range: 600 - 6000
VXLAN GPE Tunnel UDP Source Port Range: 400 - 4000
VXLAN Dummy L2 Tunnel UDP Source Port Range: 1025 - 65535
VXLAN GPE Tunnel UDP Source Port Hash: 5 tuples
VXLAN  Dummy L2 Tunnel UDP Source Port Hash: 5 tuples
```

Additional References for VxLAN GPE Tunnel and VxLAN Dummy-L2 Tunnel

Standards and RFCs

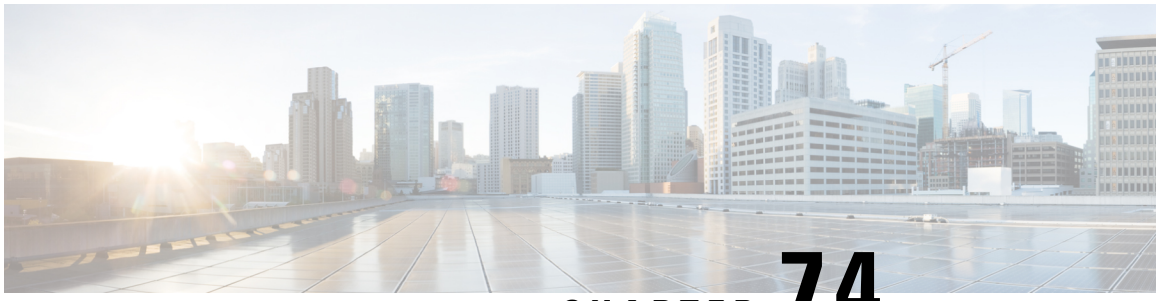
Standard/RFC	Title
draft-ietf-nvo3-vxlan-gpe-02.txt	*Generic Protocol Extension for VXLAN*

MIBs

MIB	MIBs Link
• CISCO-VXLAN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 74

EVPN VxLAN L3

This chapter provides information on Layer 3 Data-Center-Interconnect (DCI) VXLAN EVPN Support.

Feature Information for EVPN VxLAN L3

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 96: Feature Information for EVPN VxLAN L3

Feature Name	Releases	Feature Information
EVPN VxLAN L3	Cisco IOS XE Denali 16.3.1	The EVPN VxLAN L3 is a new feature.
VXLAN EVPN Fabric DCI - MPLS L3VPN	Cisco IOS XE Everest 16.4.1	The VXLAN EVPN Fabric DCI - MPLS L3VPN is a new feature.
VXLAN EVPN External Connectivity	Cisco IOS XE Bengaluru 17.5.1	Support for IPv6 for the EVPN VxLAN L3 feature.

Restrictions for EVPN VxLAN L3

- VNI range CLI for L3VNI is not supported.
- Egress traffic stops, if local VNI is down.
- L3 VNI and L2 VNI cannot co-exist in the same bridge domain as L3 VNI is not supported.
- MAC learning is not done with L3VNI via control plane learning.
- External connectivity with VPLS networks is supported only when bridging is the mode of interworking between the two domains. Integrated routing and bridging (IRB) is not supported between a BGP EVPN VXLAN fabric and a VPLS network.
- External Connectivity with Layer 3 networks is supported only for IPv4 and IPv6 unicast traffic.
- MVPN network is not supported for multicast traffic.
- Import of EVPN IP routes, which includes route type 5 and route type 2 host which routes to the global routing table is not supported.

Information About EVPN VxLAN L3

Data Center Interconnect VXLAN Layer 3 Gateway

The Cisco device can serve as a Data Center Interconnect (DCI) L3 Gateway to provide IP connectivity between multi-tenant remote Data Center sites. The multi-tenant Data Centers use VxLAN encapsulation to carry separate tenant IP traffic. The VXLAN-enabled Data Center sites use MP-BGP EVPN control plane for distributing both Layer-2 and Layer-3 forwarding information within the site. RFC 5512 and draft-ietf-bess-evpn-inter-subnet-forwarding-00 define how MP-BGP Network Layer Reachability Information (NLRI) carries VXLAN encapsulation as well as L2/L3 forwarding information details to provide an integrated routing and bridging solution within the Data Center site.

Route Targets

For each VRF on the DCI router, there are two sets of manually configured import and export route-targets. One set of import and export route-targets is associated with the Data Center BGP neighbor that uses EVPN address-family to exchange L3 information; the other set of import and export route-targets is associated with the L3VPN BGP neighbor that use VPNv4 unicast address-family to exchange L3 information. This separation of route targets (RTs) enables the two sets of RTs to be independently configured. The DCI router effectively stitches the two set of RTs. The RTs associated with the EVPN BGP neighbor are labelled as stitching RTs. The RTs associated with the L3VPN BGP neighbor are normal RTs.

A new keyword is added to the existing route-target configuration to specify the route targets to be used when doing EVPN-VXLAN related processing. The base (existing) route target configuration does not affect EVPN-VXLAN related processing. You can have the same RT values for both base and VxLAN routes.

Local VPNv4 Routes Advertisement

On the DCI router, the locally sourced VPNv4 routes can be advertised to the BGP EVPN neighbors with the normal route targets (RTs) configured for the VRF or the stitching RTs associated with the BGP EVPN neighbors. By default, these routes are advertised with the normal route targets.

Note You cannot configure the advertise command for VPNv4 or VPNv6 neighbors. RTs can be applied only to the sourced routes and routes learned from VRF neighbors.

Data Center VXLAN with Support for MP-BGP

The Data Center VXLAN uses MP-BGP for control-plane learning of end-host Layer 2 and Layer 3 reachability information. The DCI router is configured with a VXLAN Tunnel EndPoint (VTEP). You also need to run the host-reachabilty protocol BGP command to specify that control-plane learning within Data center site is through BGP routing protocol.

The DCI Gateway router and the EVPN BGP neighbor (Data Center BGP neighbor) exchange BGP EVPN NLRIs of route type 5 that carry L3 routing information and associated VXLAN encapsulation information.

EVPN Route Targets

A new keyword is added to the existing route-target configuration to specify the route targets to be used when doing EVPN-VXLAN related processing. The base (existing) route target configuration does not affect EVPN-VXLAN related processing. You can have the same RT values for both base and vxlan routes

MAC/IP Advertisement Route and IP Prefix Route is supported. The l2vpn evpn address-family can be configured and neighbors can exchange EVPN NLRI. The l2vpn-evpn-prefix-advertisement is supported fully and for the non-MAC portions only the NLRI is supported. IP Prefix route type is added to carry IP prefixes. The IP Prefix NLRI can carry IPv4 Prefix or IPv6 Prefix. The NLRI length determines whether it has IPv4 Prefix or IPv6 Prefix.

NLRI Format:

```
[Type][Len][RD][ESI][ETag][IP Addr Mask][IP Addr][GW IP Addr][Label]
```

Key:

```
[Type][ETag][IP Addr Len][IP Addr]
```

When BGP attribute, encapsulation type EXTCOMM value of 0x8 (VxLAN) is present, then Label carries VNI (VXLAN ID).

EVPN RT5 and RT2 that contain a RT matching an import “stitching RT” specified in a vrf configuration is accepted by the router and imported into the corresponding BGP L3VPN vrf. The resulting L3VPN prefix retains the same route target. L3VPN routes that are imported into EVPN via “advertise l2vpn evpn” contains route targets specified by that vrf’s export “stitching RT”. Any original route targets is removed.

Bridge Domain Interface

Bridge Domain Interface (BDI) is used for Inter-VLAN routing for EVC. It supports ping from local BDI interface to peer BDI/BVI/SVI. ARP is not used to resolve adjacency. BGP is asked to advertise the BDI IP address in EVPN route and use RMAC as an adjacency.

Downstream VNI

A downstream VNI is assigned at the downstream BGP peer. The BGP peer sends VNI as part of EVPN route type 2 or 5, so that it can use the VNI to send EVPN traffic to peer. This VNI is called as egress VNI; this egress VNI is used to send EVPN traffic to peer on data path. BGP also sends the local VNI to peer as part of EVPN route type 2 or 5 and it is expected from the peer to send EVPN traffic with the VNI, so that it can route the PKT to right VRF. This VNI is called as ingress VNI.

For the local VNI, VNI number range is 4k to 16m. For the egress VNI, valid VNI number range can be any valid VNI number, from 1-16m.

Router MAC

EVPN introduces a Router's MAC extended community to exchange Router's MAC between EVPN peer. BGP send BDI's MAC address to EVPN Peer as its RMAC. By default, all the BDI interface share the same MAC address, so all EVPN VRF will send the same RMAC to EVPN peer by default. It is flexible to configure MAC address of BDI interface. So, it is possible that different EVPN VRF may send different RMAC to EVPN peer.

VRF Lite

VRF-lite (VPN routing/forwarding) allows a service provider to support two or more VPNs with overlapping IP addresses. VRF-lite is achieved by configuring sub-interfaces (VLANs) on a physical interface and by putting each sub-interface in a VRF.

EVPN Route Type 2 - MAC Advertisement Route

MAC Advertisement Route can be used to carry only MAC Address or MAC Address and IP Address (/32 for IPv4 or /128 for IPv6).

NLRI Format:

```
[Type][Len][RD][ESI][ETag][MAC Addr Mask][MAC Addr][IP Addr Len][IP Addr] [Label1] [Label2]
```

Key:

```
[Type][ETag][MAC Addr Len][MAC Addr][IP Addr Len][IP Addr]
[Type][ETag][MAC Addr Len][MAC Addr][IP Addr Len]
```

Label1 is associated with MAC Address and Label2 is associated with IP Address. When BGP attribute, encapsulation type EXTCOMM value of 0x8 (VxLAN) is present, then Label carries VNI (VXLAN ID).

L3 VRF EVPN Import

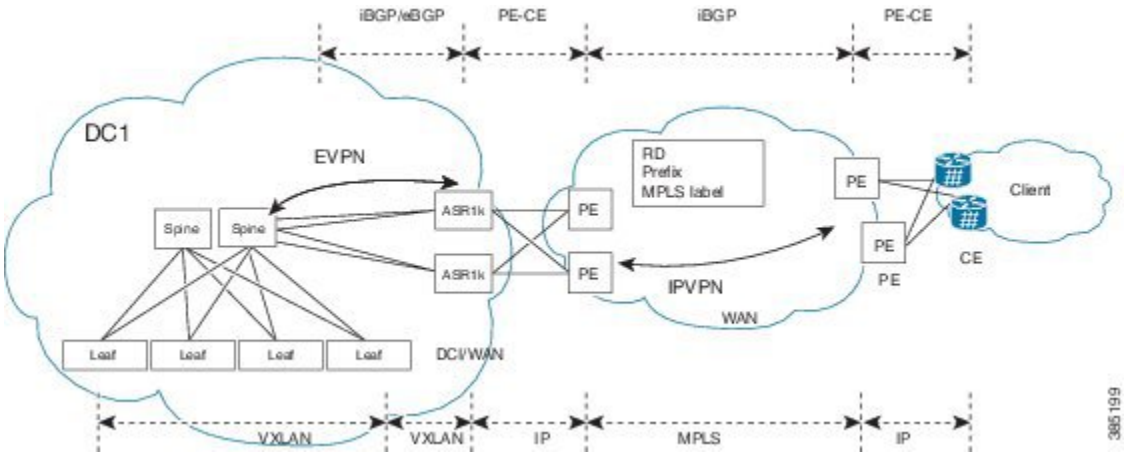
To advertise L3 VPN routing and forwarding (VRF) prefixes to EVPN neighbors define a new import type that takes prefixes from VRF neighbors, redistributed VRF routes, and import them into EVPN table. The import of VRF routes is controlled per VRF. The import of VRF is performed only when `advertise l2vpn evpn` is configured under that VRF and local VTEP is up.

EVPN DCI Solution

ASR1000 (IOS-XE Platform) series routers, acting as a Data Centre Interconnect (DCI) device can be deployed at the edge of two Cisco Data Center solutions, that is, Nexus 9000 Standalone-mode Data Centre or Nexus 9000 ACI-mode Data Centre. It provides flexible and safe WAN connections to the Internet or Branch sites with multiple different WAN types. Currently ASR1000 supports multiple WAN connection types, including iWAN, MPLS VPN(PE and ASBR), DMVPN, and VRF Lite. You can also deploy more than one ASR1000 router as multihoming deployment, if you require traffic load balancing, redundancy or customized path selection policy based on special requirements of different applications.

How to Configure EVPN VxLAN L3

The following is the sample topology that is used as an example to explain the configuration of this feature.



Configuring Customer Edge (CE) 1 Using VRF Lite

1. Define VRF and IPv4 address family. EVPN RT is 65535:1

```
vrf definition evpn1
 rd 65535:1
 address-family ipv4
route-target both 65535:1 stitching
exit-address-family
!
```

2. Define Bridge Domain and associate vxlan vni 3000.

```
bridge-domain 200
 member vni 30000
```

```
Interface loopback0
  ip address 33.33.33.33 255.255.255.255
```

3. Define Bridge Domain Interface (BDI).

```
interface BDI200
 vrf forwarding evpn1
 ip address 100.1.1.1 255.255.255.0
 encapsulation dot1Q 200
```

4. Create Interface NVE1.

```
Interface gi0/0/0.2
  enc dot1q 2
  ip address 4.0.0.1 255.255.255.0
Interface gi0/0/1.2
  enc dot1q 2
  vrf forwarding evpn1
  ip address 3.3.3.1 255.255.255.0
interface nve1
 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 30000 vrf evpn1
```

5. Define OSPF for underlay reachability.

```
Router ospf 100
  router-id 33.33.33.33
  network 33.33.33.33 0.0.0.0 area 0
  network 4.0.0.1 0.0.0.0 area 0
!
```

6. Define BGP and EVPN address-family.

```
router bgp 65535
 bgp router-id 33.33.33.33
 neighbor 44.44.44.44 remote-as 65535
 neighbor 44.44.44.44 update-source Loopback0
 !
 address-family l2vpn evpn
  neighbor 44.44.44.44 activate
  neighbor 44.44.44.44 send-community both
 exit-address-family
 !
 address-family ipv4 vrf evpn1
  advertise l2vpn evpn
  neighor 3.3.3.254 remote-as 65530
  neighor 3.3.3.254 update-source Gi0/0/1.2
  neighor 3.3.3.254 ebgp-multihop 255
  redistribute connected
 exit-address-family
```

Configuring Provider Edge 1

Define VRF and RD/RT.

```
vrf definition vrf1
 rd 65530:1
 address-family ipv4
  route-target both 65530:1
exit-address-family
!
interface loopback0
```

```
  ip address 33.33.33.22 255.255.255.255
Interface GigabitEthernet0/0/0.2
  enc dot1q 2
  vrf forwarding vrf1
  ip address 3.3.3.254 255.255.255.0
Interface gigabitEthernet0/0/1
  mpls ip
  ip address 2.2.2.1 255.255.255.0
!
Router ospf 100
  router-id 33.33.33.22
  network 33.33.33.22 0.0.0.0 area 0
  network 2.2.2.1 0.0.0.0 area 0
!

router bgp 65530
 bgp router-id 33.33.33.22
 neighbor 22.22.22.22 remote-as 65530
 neighbor 22.22.22.22 update-source Loopback0
 !
 address-family vpnv4
  neighbor 22.22.22.22 activate
  neighbor 22.22.22.22 send-community both
 exit-address-family
 !
 address-family ipv4 vrf vrf1
  neighor 3.3.3.253 remote-as 65535
  neighor 3.3.3.253 update-source Gi0/0/0.2
  neighor 3.3.3.253 ebgp-multihop 255
  redistribute connected
 exit-address-family
```

Configuring Provider Edge 2 and Branch Router

```
vrf definition vrf1
 rd 65530:1
 address-family ipv4
  route-target both 65530:1
exit-address-family
!
interface loopback0
  ip address 22.22.22.22 255.255.255.255
!
Interface GigabitEthernet0/0/0.200
  enc dot1q 200
  vrf forwarding vrf1
  ip address 1.1.1.254 255.255.255.0
!
Interface gigabitEthernet0/0/1
  mpls ip
  ip address 2.2.2.254 255.255.255.0
!
Router ospf 100
  router-id 22.22.22.22
  network 22.22.22.22 0.0.0.0 area 0
  network 2.2.2.254 0.0.0.0 area 0
!

router bgp 65530
 bgp router-id 22.22.22.22
 neighbor 33.33.33.22 remote-as 65530
 neighbor 33.33.33.22 update-source Loopback0
 !
 address-family vpnv4
```

```
 neighbor 33.33.33.22 activate
 neighbor 33.33.33.22 send-community both
exit-address-family
!
address-family ipv4 vrf vrf1
  redistribute connected
exit-address-family
```

Configuring Customer Edge 2

```
Interface GigabitEthernet0/0/0.200
  enc dot1q 200
ip address 1.1.1.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 1.1.1.254
```

Importing Between EVPN and VRF/VPN

```
router bgp 100
 address-family ipv4 vrf example-vrf
  advertise l2vpn evpn
  neighbor 7.7.7.7 remote-as 400
  neighbor 7.7.7.7 activate
 exit-address-family
```

Configure EVPN VxLAN Handoff

External connectivity or handoff refers to the movement of Layer 2 and Layer 3 traffic between an EVPN VXLAN network and an external network. This connectivity enables the EVPN VXLAN network to exchange routes with the externally connected network.

The EVPN VXLAN network imports the reachability routes from the external network and extends the Layer 2 or Layer 3 overlay network outside the VXLAN network. The process of extending a Layer 2 or Layer 3 network outside the EVPN VXLAN network is also known as handoff.

The following procedures tell you how to configure the external handoff between an EVPN VXLAN network and an external layer 2 or a layer 3 network. To enable the EVPN VLAN Layer 3 external handoff with an MPLS Layer 3 VPN network:

1. Run the **mpls label mode all-vrfs protocol all-afs per-vrf** command in the global configuration mode on the border VTEP.
2. Configure BGP with with a new route type for Layer 2 VPN, VPNv4, VPNv6 address families on the border VTEP.
3. Configure BGP on the border VTEP for external connectivity with the MPLS Layer 3 VPN.

Configuration on the EVPN VxLAN Fabric

Run the following configuration on the EVPN VxLAN fabric. Here, the EVPN routes imported from the EVPN fabric into the VPNv4 address family as VPNv4 routes and distributes them to the external network.

```
vrf definition evpn0
 rd 65535:4000
```

```
 !
 address-family ipv4
  route-target export 65535:1
  route-target import 65535:1
  route-target export 65535:1 stitching
  route-target import 65535:1 stitching
 exit-address-family
!
 address-family ipv6
  route-target export 65535:1
  route-target import 65535:1
  route-target export 65535:1 stitching
  route-target import 65535:1 stitching
  exit-address-family
!
interface GigabitEthernet3
 ip address 10.0.4.1 255.255.255.0
!
interface Loopback0
 ip address 4.4.4.1 255.255.255.255
!
interface BDI200
 vrf forwarding evpn0
 ip address 150.1.1.1 255.255.255.0
 ipv6 address 2000::150:1:1:1/112
interface nve1
 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 50000 vrf evpn0
!
bridge-domain 200
 member vni 50000
!
router bgp 65535
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 6.6.6.1 remote-as 1
 neighbor 6.6.6.1 ebgp-multihop 3
 neighbor 6.6.6.1 update-source Loopback0
 !
 address-family l2vpn evpn
  neighbor 6.6.6.1 activate
  neighbor 6.6.6.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf evpn0
  advertise l2vpn evpn
  redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf evpn0
  redistribute connected
  advertise l2vpn evpn
 exit-address-family
!
router ospf 10
 nsf cisco
 network 4.4.4.1 0.0.0.0 area 0
 network 10.0.4.1 0.0.0.0 area 0
```

Configuration on the Border Node

Perform the following configuration on the border node. Here, the lsvpn evpn re-originate command imports the EVPN route into VPNv6 address family and carried over L3-VPN MPLS network.

The import vpnv4 unicast and the vpnv6 unicast commands enable the import of the VPN route into the EVPN table.

```
vrf definition evpn0
 rd 65535:6000
 !
 address-family ipv4
  route-target export 65535:1
  route-target import 65535:1
  route-target export 65535:1 stitching
  route-target import 65535:1 stitching
 exit-address-family
!
 address-family ipv6
  route-target export 65535:1
  route-target import 65535:1
  route-target export 65535:1 stitching
  route-target import 65535:1 stitching
 exit-address-family
!
bridge-domain 200

 member vni 40000

!
interface Loopback0

 ip address 6.6.6.1 255.255.255.255

!

interface Loopback10

 ip address 60.60.60.1 255.255.255.255
!
interface GigabitEthernet2
 ip address 10.0.4.2 255.255.255.0
!
interface GigabitEthernet4
 ip address 102.2.2.2 255.255.255.0
 ip ospf 1 area 0
 mpls ip
!
interface BDI200
 vrf forwarding evpn0
 ip address 200.1.1.1 255.255.255.0
 ipv6 address 2000::200:1:1:1/112
!
interface nve1

 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 40000 vrf evpn0
!
router bgp 1

 bgp log-neighbor-changes
```

```
bgp graceful-restart
no bgp default ipv4-unicast
neighbor 4.4.4.1 remote-as 65535
neighbor 4.4.4.1 ebgp-multihop 3
neighbor 4.4.4.1 update-source Loopback0
neighbor 8.8.8.1 remote-as 1
neighbor 8.8.8.1 update-source Loopback10
!
address-family ipv4
exit-address-family
!
address-family vpnv4
 import l2vpn evpn re-originate
 neighbor 8.8.8.1 activate
 neighbor 8.8.8.1 send-community both
 neighbor 8.8.8.1 next-hop-self all
exit-address-family
!
address-family ipv6
exit-address-family
!
address-family vpnv6
 import l2vpn evpn re-originate
 neighbor 8.8.8.1 activate
 neighbor 8.8.8.1 send-community both
 neighbor 8.8.8.1 next-hop-self
exit-address-family
!
address-family l2vpn evpn
 import vpnv4 unicast
 import vpnv6 unicast
 neighbor 4.4.4.1 activate
 neighbor 4.4.4.1 send-community both
```

```
 exit-address-family

 !

 address-family ipv4 vrf evpn0

  advertise l2vpn evpn

  redistribute connected

 exit-address-family

 !
 address-family ipv6 vrf evpn0

  advertise l2vpn evpn

  redistribute connected

 exit-address-family
!
router ospf 1
 redistribute connected
 passive-interface GigabitEthernet2 !don't notify the ospf to gi2
!
router ospf 10
 nsf cisco
 passive-interface GigabitEthernet4
 network 6.6.6.1 0.0.0.0 area 0
 network 10.0.4.2 0.0.0.0 area 0
```

Configuration on the WAN Network

Perform the following configuration on the WAN network. In this BGP VPN configuration, the VPNv6 route is received from the border node and is imported into the VRF based on the VRF RT configuration. This route from the VRF is advertised as the VPN route to the remote end.

```
vrf definition evpn0
 rd 65535:8000
 !
 address-family ipv4
  route-target export 65535:1
  route-target import 65535:1
 exit-address-family
!
 address-family ipv6
  route-target export 65535:1
  route-target import 65535:1
 exit-address-family

!
interface Loopback0

 ip address 8.8.8.1 255.255.255.255
!
interface Loopback10
 vrf forwarding evpn0

 ip address 58.1.1.1 255.255.255.255
 ipv6 address 2000::58:1:1:1/128
!
```

```
interface GigabitEthernet2

 ip address 102.2.2.1 255.255.255.0

 ip ospf 1 area 0

 speed 1000

 mpls ip
!
router bgp 1

 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 60.60.60.1 remote-as 1

 neighbor 60.60.60.1 update-source Loopback0

 !
address-family vpnv4
  neighbor 60.60.60.1 activate

  neighbor 60.60.60.1 send-community both

  neighbor 60.60.60.1 route-reflector-client

  neighbor 60.60.60.1 next-hop-self

 exit-address-family

 !

 address-family vpnv6

  neighbor 60.60.60.1 activate

  neighbor 60.60.60.1 send-community both

  neighbor 60.60.60.1 route-reflector-client

 exit-address-family

 !

 address-family ipv4 vrf evpn0

  redistribute connected  ! redistribute local network to evpn

  redistribute static  ! redistribute static route to evpn

 exit-address-family
!
 address-family ipv6 vrf evpn0
  redistribute connected
  redistribute static
 exit-address-family
!
router ospf 1
 nsf cisco
 redistribute connected

 network 0.0.0.0 255.255.255.255 area 0
```

-

Verifying EVPN VxLAN L3

Use the following commands to verify the configuration:

- **show ip bgp l2vpn evpn**: Displays Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table.
- **show mlrib evpn mac**: Displays the MLRIB information pertaining to an EVPN network.
- **show nve peers**: Displays information that determine if the VNI is configured for peer.

Show Command-BGP

```
#show ip bgp l2vpn evpn summary
BGP router identifier 19.0.0.1, local AS number 1
BGP table version is 2, main routing table version 2
1 network entries using 376 bytes of memory
1 path entries using 196 bytes of memory
1/1 BGP path/bestpath attribute entries using 272 bytes of memory
1 BGP extended community entries using 40 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 884 total bytes of memory
BGP activity 1/0 prefixes, 1/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
20::46          4            1    7852    7849        2    0    0 4d22h           0
19.0.101.1      4            1       0       0        1    0    0 never    Idle
19.0.101.2      4            1       0       0        1    0    0 never    Idle
19.0.101.3      4            1       0       0        1    0    0 never    Idle
19.0.101.4      4            1       0       0        1    0    0 never    Idle
19.0.101.5      4            2       0       0        1    0    0 never    Idle
19.0.101.6      4            1       0       0        1    0    0 never    Idle
19.0.101.7      4            1   80385    7853        2    0    0 4d22h           1
20.0.0.47       4            1    7857    7844        2    0    0 4d22h           0
FEC0::1001      4            1       0       0        1    0    0 never    Idle
```

Show Command-MLRIB

```
# show mlrib evpn mac
EVI   MAC Address  Owner Next-Hop  iVNI  eVNI
-----------------------------------------------------
100   aaa.bbb.cc1   NVE   1.2.3.4   10000 1000

# show mlrib evpn mac detailed
EVI MAC Address Owner Next-Hop  iVNI  eVNI lVTEP     port
-------------------------------------------------------------
100 aaa.bbb.cc1 NVE   1.2.3.4   1000  1000 1.2.3.2   2000

# show mlrib evpn vtep local
BD    RMAC Address    VTEP-IP       VRF     VNI  BDI
-----------------------------------------------------------
100   aaa.bbb.cc2    101.2.3.4      vrf1    10000    BDI100
```

Show NVE Peers

```
#sh nve peers vni 10135
Interface  VNI      Type Peer-IP          Router-RMAC    eVNI     state flags UP time
nve1       10135    L3CP 66.66.66.66      5c83.8f5f.5c97 10135      UP   A/M 00:08:53
```

Verifying EVPN VxLAN Handoff

To verify whether the external handoff is successful, run the following show commands:

Step 1 Verify EVPN by running the show evpn peers command.

a) VxLAN Fabric

```
router#show evpn peers
Intf     VNI      Type   Peer-IP          Router-RMAC    eVNI     state flags   UP time
nve1     50000    L3NVE  6.6.6.1          001e.bd6e.22bf 40000      UP  A/-/4  01:48:57
nve1     50000    L3NVE  6.6.6.1          001e.bd6e.22bf 40001      UP  A/-/4  01:48:57
nve1     50000    L3NVE  6.6.6.1          001e.bd6e.22bf 40002      UP  A/M/4  01:48:57
nve1     50000    L3NVE  6.6.6.1          001e.bd6e.22bf 40000      UP  A/-/6  01:48:57
```

b) Border Node

```
BorderRouter#show evpn peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Intf     VNI      Type   Peer-IP          Router-RMAC    eVNI     state flags   UP time
nve1     40000    L3NVE  4.4.4.1          001e.1403.63bf 50000      UP  A/-/4  01:58:36
nve1     40001    L3NVE  4.4.4.1          001e.1403.63bf 50000      UP  A/M/4  01:58:36
nve1     40002    L3NVE  4.4.4.1          001e.1403.63bf 50000      UP  A/M/4  01:58:36
nve1     40000    L3NVE  4.4.4.1          001e.1403.63bf 50000      UP  A/M/6  01:58:36
```

Step 2 Verify the BGP EVPN RT5 route by running the show bgp l2vpn evpn route-type 5 command:

a) VxLAN Fabric

```
Router#show bgp l2vpn evpn route-type 5
BGP routing table entry for [5][65535:1][0][112][2000::58:1:1:0]/29, version 10
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Not advertised to any peer
  Refresh Epoch 1
  1
    6.6.6.1 (metric 2) (via default) from 6.6.6.1 (60.60.60.1)
      Origin incomplete, localpref 100, valid, external, best
      EVPN ESI: 00000000000000000000, Gateway Address: ::, VNI Label 40000, MPLS VPN Label 0
      Extended Community: RT:65535:1 ENCAP:8 Router MAC:001E.BD6E.22BF
      rx pathid: 0, tx pathid: 0x0
      net: 0x7F3224F19DF8, path: 0x7F32250DCAE0, pathext: 0x7F31B92F7D38
      flags: net: 0x0, path: 0x3, pathext: 0x81
      attribute: 0x7F32250CD030, ref: 5
      Updated on Feb 3 2021 18:05:04 UTC
```

b) Border Node

```
BorderNode#show bgp l2vpn evpn route-type 5
...
BGP routing table entry for [5][65535:1][0][112][2000::58:1:1:0]/29, version 7
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  Local, imported path from base
    ::FFFF:8.8.8.1 (metric 2) (via default) from 8.8.8.1 (80.80.80.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000, Gateway Address: 0.0.0.0, local vtep: 6.6.6.1, VNI Label
40000, MPLS VPN Label 24
      Extended Community: RT:65535:1 ENCAP:8 Router MAC:001E.BD6E.22BF
```

```
      rx pathid: 0, tx pathid: 0x0
     net: 0x7F67C81E5128, path: 0x7F67B8AC0210, pathext: 0x7F67C8371CC0, exp_net: 0x7F67C74227F8

      flags: net: 0x0, path: 0x7, pathext: 0xA1
      attribute: 0x7F67C7661858, ref: 3
      Updated on Feb 3 2021 18:04:47 UTC
```

Step 3 Verify the BGP binding label by running the show ip bgp vpnv6 unicast vrf command:

a) VxLAN Fabric

```
Router#sh ipv6 cef vrf evpn0 2000::58:1:1:0/112 internal
2000::58:1:1:0/112, epoch 0, flags [rnolbl, rlbls], RIB[B], refcnt 5, per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00018000
    Broker: linked, distributed at 3rd priority
  ifnums:
    BDI200(26): 6.6.6.1
  path list 7F321ABA2F28, 5 locks, per-destination, flags 0x269 [shble, rif, rcrsv, hwcn, bgp]
    path 7F322454CB88, share 1/1, type recursive, for IPv6
      recursive via 50331650[Binding-Sid Label:Default], fib 7F31B6375230, 1 terminal fib,
bslbl:Default:50331650
      path list 7F321ABA3318, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
          path 7F322454D068, share 1/1, type attached nexthop, for IPv6, cid [40000]
            nexthop 6.6.6.1 BDI200, IPV6 adj out of BDI200, addr 6.6.6.1, cid: 40000 7F3224F853F8

  output chain:
    IPV6 adj out of BDI200, addr 6.6.6.1, cid: 40000 7F3224F853F8
```

```
Router# show ip bgp vpnv6 unicast vrf evpn0 2000::58:1:1:0/112 internal
BGP routing table entry for [65535:1]2000::58:1:1:0/112, version 4
Paths: (1 available, best #1, table evpn0)
Not advertised to any peer
Refresh Epoch 1
1, imported path from [5][65535:1][0][112][2000::58:1:1:0]/29 (global)
::FFFF:6.6.6.1(metric 2) (via default) from 6.6.6.1(60.60.60.1)
Origin incomplete, localpref 100, valid, external, best
Extended Community: RT:65535:1 ENCAP:8 Router MAC:001E.BD6E.22BF
Local vxlan vtep:
vrf:evpn0, vni:50000
local router mac:001E.1403.63BF
encap:8
vtep-ip:4.4.4.1
bdi:BDI200
Remote VxLAN [attr 0x7F31B8B5E9C8(Ref:7), rnh 0x7F321C245668(Ref:2)]:
Topoid 0x1E000002(vrf evpn0)
Remote Router MAC:001E.BD6E.22BF
Encap 8
Egress VNI 40000
RTEP 6.6.6.1
Binding Label: 0x3000002
rx pathid: 0, tx pathid: 0x0
net: 0x7F31B8B4E7A8, path: 0x7F31B8B7EAA8, pathext: 0x7F3224EFAA88, exp_net: 0x7F3224F19DF8
flags: net: 0x0, path: 0x7, pathext: 0x181
attribute: 0x7F31B8B5E9C8, ref: 6
Updated on Feb 3 2021 18:05:04 UTC
```

Configuring EVPN: Basic Configuration

Perform the following tasks to configure EVPN:

1. Create a VRF.

```
vrf definition EVPN
 rd 100:1
 !
 address-family ipv4
  route-target export 100:1 stitching
  route-target import 100:1 stitching
 exit-address-family
```

2. Create a bridge domain and assign a VNI.

```
bridge-domain 1234
 member vni 101234
```

3. Create a BDI interface and assign it to the EVPN VRF.

```
interface BDI1234
 vrf forwarding EVPN
 ip address 10.20.30.40 255.255.255.0
 encapsulation dot1Q 1234
```

4. Create an NVE interface.

```
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 101234 vrf EVPN

router bgp 100
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.10.10.111 remote-as 100
 neighbor 10.10.10.111 ebgp-multihop 255
 neighbor 10.10.10.111 update-source Loopback1
 neighbor 10.10.10.222 remote-as 100
 neighbor 10.10.10.222 ebgp-multihop 255
 neighbor 10.10.10.222 update-source Loopback1
 !
```

5. Configure a EVPN sessions to two spines.

```
address-family l2vpn evpn
  neighbor 10.10.10.111 activate
  neighbor 10.10.10.111 send-community both
  neighbor 10.10.10.222 activate
  neighbor 10.10.10.222 send-community both
 exit-address-family
```

Example: EVPN Interconnect With MPLS VPN as ASBR

```
router bgp 100
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
```

```
neighbor 9.9.8.8 remote-as 200
Neighbor 9.9.8.8 ebgp-multihop 255

neighbor 9.9.8.8 update-source Loopback0
!
address-family vpnv4
 import l2vpn evpn
 neighbor 9.9.8.8 activate
 neighbor 9.9.8.8 send-community extended
 neighbor 9.9.8.8 next-hop-self all
 Neighbor 9.9.8.8 inter-as-hybrid
```

Configuring Inter-AS Option AB

The following sections describe how to configure the Inter-AS Option AB feature on an ASBR for either an MPLS VPN or an MPLS VPN that supports CSC:

Note If Inter-AS Option AB is already deployed in your network and you want to do Option B style peering for some prefixes (that is, implement Inter-AS Option AB+), configure the **inter-as-hybrid global** command as described in the "Configuring the Routing Policy for VPNs that Need Inter-AS Connections" section.

Configuring the VRFs on the ASBR Interface for Each VPN Customer

Use the following steps to configure the VRFs on the ASBR interface for each VPN customer so that these VPNs have connectivity over the MPLS VPN--Inter-AS Option AB network.

Note The **mpls bgp forwarding** command is used only on the ASBR interface for VRFs that support CSC.

Use all of the steps in the following procedure to configure additional VRFs that need to be configured on the ASBR interface and the VRFs that need to be configured on the peer ASBR interface.

1. Enable privileged EXEC mode. Enter your password if prompted.

   ```
   enable
   Example:
   Router> enable
   ```

2. Enter global configuration mode.

   ```
   configure terminal
   Example:
   Router# configure terminal
   ```

3. Specify the interface to configure and enter the interface configuration mode.
   - The *type* argument specifies the type of interface to be configured.
   - The *number* argument specifies the port, connector, or interface card number.

   ```
   interface type number
   Example:
    Router(config)# interface Ethernet 5/0
   ```

4. Associate a VRF with the specified interface or subinterface.

- The *vrf-name* argument is the name assigned to a VRF.

```
ip vrf forwarding vrf-name
Example:
 Router(config-if)# ip vrf forwarding vpn1
```

5. (Optional) Configures BGP to enable MPLS forwarding on connecting interfaces for VRFs that must support MPLS traffic.
   - This step applies to a CSC network only.

```
mpls bgp forwarding
Example:
 Router(config-if)# mpls bgp forwarding
```

6. (Optional) Exits to privileged EXEC mode.

```
end
Example:
 Router(config-if)# end
```

Configuring MP-BGP Session Between ASBR Peers

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (see RFC 2283, *Multiprotocol Extensions for BGP-4*), which define support for address families other than IPv4. Using the extensions ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

Follow the steps in this section to configure the MP-BGP session on the ASBR.

Use all of the steps in the following procedure to configure the MP BGP session on the peer ASBR.

1. Enable privileged EXEC mode. Enter your password if prompted.

```
enable
Example:
Router> enable
```

2. Enter global configuration mode.

```
configure terminal
Example:
Router# configure terminal
```

3. Configures a BGP routing process and places the router in router configuration mode.
   - The *as-number* argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.

```
router bgp as-number
Example:
 Router(config)# router bgp 100
```

4. Adds an entry to the BGP or multiprotocol BGP neighbor table.
   - The *ip-address* argument specifies the IP address of the neighbor.
   - The *peer-group-name* argument specifies the name of a BGP peer group.
   - The *as-number* argument specifies the autonomous system to which the neighbor belongs.

```
neighbor {ip-address | peer-group-name} remote-as as-number
Example:
 Router(config-router)# neighbor 192.168.0.1
remote-as 200
```

5. Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
   - The **unicast** keyword specifies IPv4 unicast address prefixes.

```
address-family vpnv4 [unicast]
Example:
 Router(config-router)# address-family vpnv4
```

6. Enables the exchange of information with a neighboring router.
   - The *ip-address* argument specifies the IP address of the neighbor.
   - The *peer-group-name* argument specifies the name of a BGP peer group.

```
neighbor {ip-address | peer-group-name} activate
Example:
 Router(config-router-af)# neighbor 192.168.0.1
activate
```

7. Configures eBGP peer router (ASBR) as an Inter-AS Option AB peer.
   - The *ip-address* argument specifies the IP address of the neighbor.
   - The *peer-group-name* argument specifies the name of a BGP peer group.
   - If any prefixes are imported into Option AB VRFs, then the imported paths are advertised to this peer.
   - If any prefixes are received from this peer and are imported into Option AB VRFs, then the imported paths are advertised to iBGP peers.

Note Advertised routes have RTs that are configured on the VRF. Advertised routes do not have their original RTs.

```
neighbor {ip-address | peer-group-name} inter-as-hybrid
Example:
 Router(config-router-af)# neighbor 192.168.0.1
inter-as-hybrid
```

8. Exits from address family configuration mode.

```
exit-address-family
Example:
 Router(config-router-af)# exit-address-family
```

9. (Optional) Exits to privileged EXEC mode.

```
end
Example:
 Router(config-af)# end
```

Configuring the Routing Policy for VPNs that Need Inter-AS Connections

Use the steps in this section to configure VRFs for the VPNs that need Inter-AS connections between ASBR peers, by configuring the appropriate routing policy and Option AB configuration.

Use all of the steps in the following procedure to configure additional VPNs that need Inter-AS Option AB connectivity on this ASBR and the peer ASBR.

1. Enable privileged EXEC mode. Enter your password if prompted.

```
enable
Example:
Router> enable
```

2. Enter global configuration mode.

```
configure terminal
Example:
Router# configure terminal
```

3. Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.
   - The *vrf-name* argument is the name assigned to a VRF.

```
vrf definition vrf-name
Example:
 Router(config)# vrf definition vpn1
```

4. Creates routing and forwarding tables.
   - The *route-distinguisher* argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats:
     - 16-bit autonomous system number: your 32-bit number, for example, 101:3
     - 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1

```
rd route-distinguisher
Example:
 Router(config-vrf)# rd 100:1
```

5. Enters VRF address family configuration mode to specify an address family for a VRF.
   - The **ipv4** keyword specifies an IPv4 address family for a VRF.

```
address-family ipv4
Example:
Router(config-vrf)# address-family ipv4
```

6. Creates a route-target extended community for a VRF.
   - The **import** keyword imports routing information from the target VPN extended community.
   - The **export** keyword exports routing information to the target VPN extended community.
   - The **both** keyword imports routing information from and exports routing information to the target VPN extended community.
   - The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.

```
route-target {import | export | both}
route-target-ext-community
```

```
Example:
 Router(config-vrf-af)# route-target import
100:1
```

7. For Inter-AS Option AB+, go to Step 10; otherwise, go to Step 8.
8. Specifies the VRF as an Option AB VRF, which has the following effects:
   - Routes imported to this VRF can be advertised to Option AB peers and VPNv4 iBGP peers.
   - When routes received from Option AB peers and are imported into the VRF, the next hop table ID of the route is set to the table ID of the VRF.
   - If the **csc** keyword is not used, a per-VRF label is allocated for imported routes.
   - When routes are received from Option AB peers and are imported next into the VRF, the learned out label can be installed only in forwarding when the **csc** keyword is used.

   The **csc** keyword implies the following:
   - A per-prefix label is allocated for imported routes.
   - For routes received from Option AB peers that are imported into the VRF, the learned out label is installed in forwarding.

```
inter-as-hybrid [csc]
Example:
 Router(config-vrf-af)# inter-as-hybrid
```

9. (Optional) Specifies the next hop IP address to be set on paths that are imported into the VRF and that are received from an Option AB peer.
   - The next hop context is also set to the VRF, which imports these paths.
   - The **csc** keyword implies the following:
     - A per-prefix label is allocated for imported routes.
     - For routes received from Option AB peers that are imported into the VRF, the learned out label is installed in forwarding.

```
inter-as-hybrid next-hop global
Example:
 Router(config-vrf-af)# inter-as-hybrid next-hop
global
```

10. (For Option AB+) Enables Inter-AS Option AB+.
    - Specifies that the next-hop address for BGP updates to be set on paths that are imported to the VRF and that are received from an Option AB+ peer are placed in the global routing table.
    - The address used is the address of the interface that is at the remote end of the external BGP (eBGP) global shared link. The next-hop context is retained as global and not modified to that of the importing VRF.

```
inter-as-hybrid next-hop global
Example:
 Router(config-vrf-af)# inter-as-hybrid next-hop
global
```

11. (Optional) Exits to privileged EXEC mode.

```
end
Example:
 Router(config-vrf-af)# end
```

Example: EVPN Interconnect With MPLS VPN as ASBR

```
router bgp 100
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 9.9.8.8 remote-as 200
 Neighbor 9.9.8.8 ebgp-multihop 255

 neighbor 9.9.8.8 update-source Loopback0
 !
 address-family vpnv4
  import l2vpn evpn
  neighbor 9.9.8.8 activate
  neighbor 9.9.8.8 send-community extended
  neighbor 9.9.8.8 next-hop-self all
  Neighbor 9.9.8.8 inter-as-hybrid
```

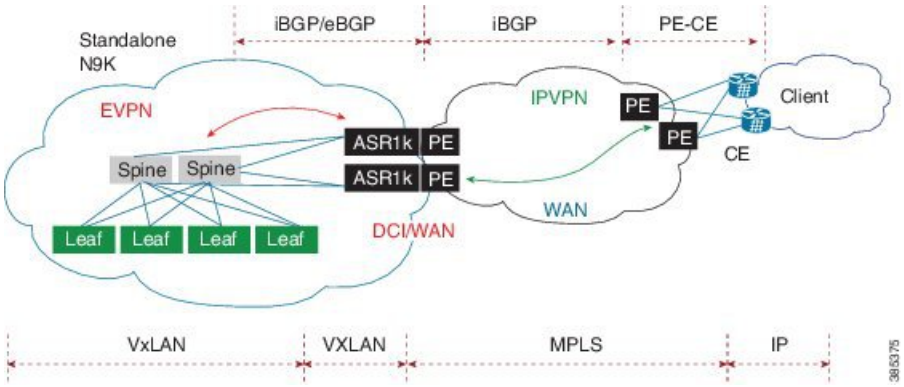
Configuring EVPN Interconnect With MPLS VPN as PE

ASR1000 supports direct prefix redistribution between BGP VPNv4 and BGP L2VPN EVPN address families. ASR1000 can act as gateway of Data Centre network and PE of MPLS VPN network both. It receives MPLS VPN prefixes from P/PE routers and these prefixes can be imported into BGP EVPN rib and then forwarded to DC's spine via BGP EVPN session. It can also import BGP EVPN prefixes sent by spine into BGP VPNv4 rib and send to P/PE in MPLS VPN network. During the prefixes redistribution, ASR1k set itself as the next-hop of the prefix before sending update to its neighbors.

In this release (16.4.1), ASR1000 only supports only bi-directional redistribution between EVPN and VPNv4. Redistribution between EVPN and VPNv6 is not supported.

In the scenario explained in the below figure shows, ASR1k acting as a PE in the MPLS-VPN network. Firstly, VRF is needed for the EVPN RT-5 routes to be imported, and then re-originate as VPN route into the MPLS-VPN side. VPN route that is learnt from the MPLS-VPN side will then first be imported into VRF, and the re-originated into EVPN as RT-5 routes.

Figure 40: EVPN Interconnect With MPLS VPN as PE



1. Define VRF and IPv4 address family.

```
vrf definition EVPN
 rd 100:1
 !
 address-family ipv4
  route-target import 100:1
  route-target import 100:1
  route-target export 100:1 stitching
  route-target import 100:1 stitching
 exit-address-family
!
```

2. Configure interface Loopback0.

```
interface Loopback0
MPLS VPN
 ip address 9.9.10.10 255.255.255.255
 ip router isis vpn
 Ip ospf 100 area 0
!
```

3. Configure interface GigabitEthernet.

```
interface GigabitEthernet0/0/0
facing MPLS VPN P/PE
 ip address 9.9.108.10 255.255.255.0
 ip router isis vpn
 negotiation auto
 mpls ip
cdp enable
!
Interface gi0/0/1.4
  Description facing to ACI spine
 Encapsulation dot1q 4
  Ip address 10.10.10.1 255.255.255.0
  Ip ospf 100 area 0
```

4. Create Interface NVE1.

```
interface nve1
 no ip address
 source-interface Loopback0
 host-reachability protocol bgp
 member vni 101234 vrf EVPN
!
```

5. Configure bridge domain.

```
Bridge-domain 100
  Member vni 101234
Interface bdi100
  Vrf forwarding EVPN
   Encapsulation dot1q 100
 Ip address 9.10.0.1 255.255.255.0

Router ospf 100
  Router-id 9.9.10.10
  Area 0.0.0.100 nssa

router isis vpn
 net 49.0001.1010.1010.1010.00
 is-type level-2-only
 metric-style wide
!
```

6. Define BGP and EVPN address-family.

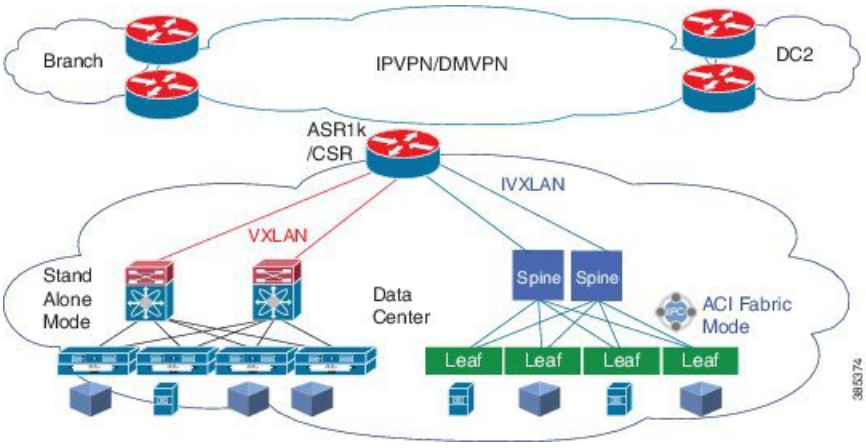
```
router bgp 200
 bgp router-id 10.10.10.10
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 9.9.8.8 remote-as 200
 neighbor 9.9.8.8 update-source Loopback0
 neighbor 10.10.10.111 remote-as 100
 neighbor 10.10.10.111 ebgp-multihop 255
 neighbor 10.10.10.111 update-source Loopback0
 neighbor 10.10.10.222 remote-as 100
 neighbor 10.10.10.222 ebgp-multihop 255
 neighbor 10.10.10.222 update-source Loopback0
 !
 address-family vpnv4
  import l2vpn evpn
  neighbor 9.9.8.8 activate
  neighbor 9.9.8.8 send-community extended
  neighbor 9.9.8.8 next-hop-self all
 exit-address-family
 !
 address-family l2vpn evpn
  import vpnv4 unicast
  neighbor 10.10.10.111 activate
  neighbor 10.10.10.111 send-community both
  neighbor 10.10.10.222 activate
  neighbor 10.10.10.222 send-community both
 exit-address-family
 !
```

7. Define VXLAN UDP port.

```
vxlan udp port 0xBEEF
```

Configuring DCI EVPN Peer to ACI Spine

Figure 41: DCI EVPN Peer to ACI Spine



1. Configure interface.

```
Interface gi0/0/1.4
  Description facing to ACI spine
 Encapsulation dot1q 4
  Ip address 10.10.10.1 255.255.255.0
```

```
  Ip ospf 100 area 0
```

2. Configure bridge domain.

```
Bridge-domain 100
  Member vni 101234
Interface bdi100
  Vrf forwarding EVPN
   Encapsulation dot1q 100
 Ip address 9.10.0.1 255.255.255.0

Router ospf 100
  Router-id 9.9.10.10
  Area 0.0.0.100 nssa
vxlan udp port 0xBEEF
```

Additional References for EVPN VxLAN L3

MIBs

MIB	MIBs Link
• CISCO-VXLAN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

CHAPTER 75

Information About Layer 2 EVPN VXLAN

Border Gateway Protocol (BGP) Ethernet VPN (EVPN) Virtual Extensible LAN (VXLAN) is a campus and data center network solution for Cisco devices running Cisco IOS XE software. It is designed to provide a unified overlay network solution.

VXLAN is a MAC in IP/UDP overlay that allows Layer 2 segments to be stretched across an IP core. All the benefits of Layer 3 topologies are thereby available with VXLAN. The encapsulation and decapsulation of VXLAN headers is handled by a functionality embedded in VXLAN Tunnel End Points (VTEPs). VTEPs themselves can be implemented in a software or a hardware form factor.

VXLAN natively operates on a flood and learn mechanism where Broadcast, unknown-unicast and multicast (BU) traffic and Layer 2 Multicast traffic in a given VXLAN network is sent over the IP core to every VTEP that has membership in that network. IP multicast is used to send traffic over the network. The receiving VTEPs decapsulate the packet, and based on the inner frame, perform Layer 2 MAC learning. The inner Source MAC is learnt against the outer Source IP Address (SIP) corresponding to the source VTEP. In this way, reverse traffic can be unicasted toward the previously learnt end host.

One of the biggest limitations of VXLAN flood and learn is the inherent flooding that is required to ensure that learning happens at the VTEPs. In a traditional deployment, a Layer 2 segment is represented with a VLAN that comprises a broadcast domain, which also scopes BU traffic. With VXLAN, the Layer 2 segment spans a much larger boundary across an IP core where floods are translated to IP multicast. Consequently, the flood and learn based scheme presents serious scale challenges, especially as the number of end hosts go up. This is addressed through learning using a control plane for distribution of end-host addresses. The control plane of choice is BGP EVPN. BGP EVPN VXLAN modes come with integrated routing and bridging (IRB) capabilities. Depending on the subnets in which the hosts are configured, EVPN over VXLAN operates in two modes:

- Bridged Mode:EVPN over VXLAN operates in Bridged mode when the hosts are in the same subnet. Intra-subnet trafffic moves seamlessly as it involves only a Layer 2 MAC lookup.
- Routed Mode: EVPN over VXLAN operates in Routed mode when the hosts are in different subnets. Inter-subnet traffic involves Layer 2 MAC lookups and Layer 3 IP lookups.

This chapter provides a background for the evolution of the solution and covers conceptual information and basic terminology that is required to understand BGP EVPN VXLAN. Later chapters of this configuration guide include information about configuration, implementation, functionalities, and troubleshooting BGP EVPN VXLAN.

Note This feature is supported only on Cisco ASR 1000 Series, Cisco Catalyst 8500 Edge Series platforms, and Cisco Catalyst 8000V Edge platform.

Benefits of Deploying Overlay-Underlay Architecture using BGP EVPN VXLAN

Deploying an overlay-underlay architecture using BGP EVPN VXLAN provides the following advantages:

- Scalability: VXLAN provides Layer 2 connectivity that allows the infrastructure that can scale to 16 million tenant networks. It overcomes the 4094-segment limitation of VLANs. This is necessary to address today's multitenant cloud requirements.
- Flexibility: VXLAN allows workloads to be placed anywhere, along with the traffic separation required in a multitenant environment. Traffic separation is done using network segmentation (segment IDs or virtual network identifiers [VNIs]).Workloads for a tenant can be distributed across different physical devices (becouse workloads are added as the need arises, into the available server space), but the workloads are identified by the same Layer 2 or Layer 3 virtual network instance (VNI) as the case may be.
- Mobility: VMs can be moved from one data center location to another without updating spine switch tables. This is because entities within the same tenant network in a EVPN VXLAN fabric setup retain the same segment ID, regardless of their location.

Limitations for BGP VXLAN EVPN

In Cisco IOS XE Release 17.11.1, the following limitations for BGP VXLAN EVPN are applicable only on Cisco ASR 1000 Series, Cisco Catalyst 8500 Edge Series platforms, and Cisco Catalyst 8000V Edge platform:

- EVPN multihoming is not supported.
- EVPN VXLAN IPV6 underlay is not supported.
- Tenant Routed Multicast (TRM) features are not supported.
- EVPN MAC address and IP learning from a static IPv4 ARP alias entry is supported. However, similar function for IPv6 ND is not supported.

Supported Features

Cisco IOS XE Release 17.11.1 supports the following features:

- Distributed Anycast Gateway IP and MAC
- EVI (MAC-VRF)
- Local VLAN bridging
- Cross Leaf VLAN over Layer 2 VNI
- IRB (IP-VRF)
- Local across BDI Layer 3 Routing
- Cross-node Routing Over Layer 3 VNI
- MAC Learing
  - Data Plane: Local MAC and IP learning
  - Control Plane: BGP EVPN route type 2
- IP Mobility Detection for Host and Virtual Machine (VM) Move
- MAC Mobility Detection for Host and VM Move
- Address Resolution Protocol (ARP) and Neighbor Discovery Suppression
- BGP EVPN IP Prefix Route Type 5
- Ingress Replication
- Underlay Multicast Replication
- BD-VIF Support on Layer 2 EVPN
- Layer 2 EVPN without EFP Interfaces and BDI Interface
- MAC and IP Addressing learning from a static ARP alias entry

Fundamental Concepts of BGP EVPN VXLAN

This section provides information about the various fundamental concepts and terminologies that are involved in the working of BGP EVPN VXLAN.

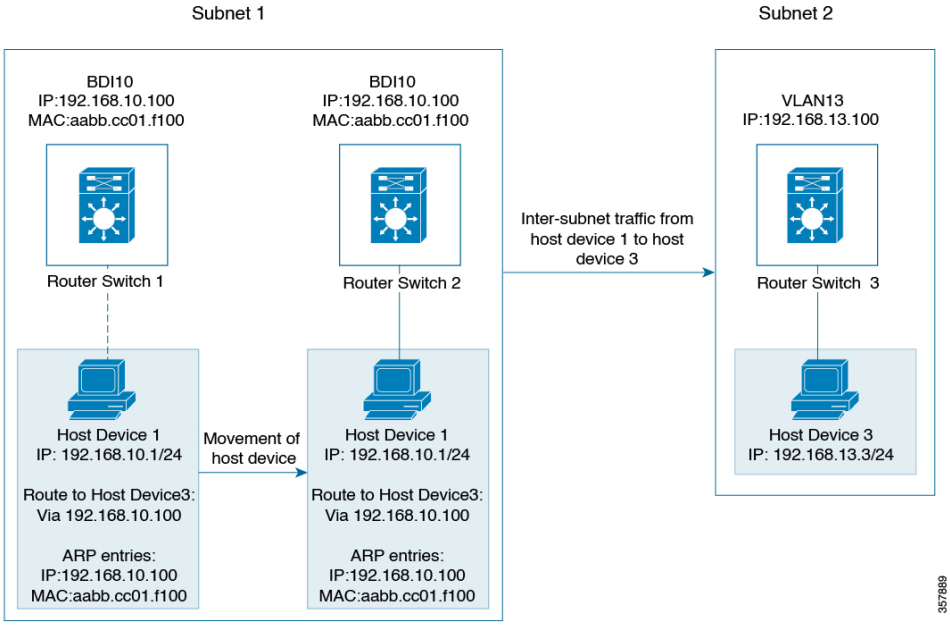
EVPN VXLAN Distributed Anycast Gateway

Distributed Anycast Gateway (DAG) is a Default-gateway Addressing (DAC) mechanism in a BGP EVPN VXLAN fabric. This feature enables the use of the same gateway IP address and MAC address across all the VETPs in an EVPN VXLAN network. This ensures that every VTEP functions as the default gateway for the workloads directly connected to it. This feature facilitates flexible workload placement, host mobility, and optimal traffic forwarding across the BGP EVPN VXLAN fabric.

The scenario shown in the figure 1 depicts a distributed gateway. Subnet 1 contains two leaf nodes—leaf node 1 and leaf node 2, acting together as a distributed default gateway for VLAN 10. Host device 1 is connected to leaf node 1 and sends traffic to host device 3, which is in a different subnet. When host device 1 tries to send traffic outside of subnet 1, the traffic goes through the configured gateway in leaf node 1. Host device 1 registers the Address Resolution Protocol (ARP) entries of the gateway VLAN MAC and IP address in leaf node 1.

When multiple VETPs act together as a single distributed default gateway for the same VLAN, the VLAN IP address remains the same across all of them. This IP address becomes the gateway IP address for any host device in the VLAN that tries to reach an IP address outside its subnet. But, each VTEP retains its own MAC address.

Figure 42: An EVPN VXLAN Network with Distributed Gateway



In the preceding figure, consider a scenario where host device 1 moves from leaf node 1 to leaf node 2. The host device remains within the same network and maintains the same ARP entries for gateway MAC addresses and IP addresses. But the MAC addresses of the VLAN interfaces in leaf node 2 and leaf node 1 are different. This results in a MAC address mismatch between the ARP entry and the VLAN on leaf node 2. As a result, any traffic that Host device 1 tries to send outside of Subnet 1 is either lost or continuously flooded as unknown unicast. The EVPN VXLAN Distributed Anycast Gateway feature prevents this traffic loss by ensuring that all the VTEPs have the same gateway MAC addresses and IP addresses in BDI.

Manual MAC address configuration and MAC aliasing are the two methods used to maintain the same MAC address across all the VTEPs and configure distributed anycast gateway.

EVPN VXLAN Centralized Gateway

In Centralized Gateway (CGW), the network has a CGW VTEP that performs the Layer 3 gateway function for all the Layer 2 VNIs. All the other VTEPs in the network perform only bridging. The CGW VTEP acts as the Layer 3 gateway and performs routing for the intersubnet VXLAN traffic.

The CGW VTEP advertises the BDI MAC-IP route for a particular VXLAN-enabled VLAN to all other Layer 2 VTEPs that have the same Layer 2 VNI configured. This allows the VTEPs to import and install the remote BDI MAC-IP route as a VXLAN Layer 3 gateway address. A host device uses the address of a BDI in the same VLAN on the CGW VTEP as its gateway address. Configure the BDI for the Layer 2 VNI VLAN only on the CGW VTEP. Do not configure the BDI (for the respective Layer 2 VNI VLAN) on any other VTEP in the network that acts as a Layer 2 VTEP.

When a host device connected to a Layer 2 VTEP sends traffic to a different subnet, the traffic is bridged from the Layer 2 VTEP to the CGW VTEP. The CGW VTEP then routes the traffic to the destination subnet. The destination subnet can be another VXLAN-enabled VLAN or an external route.

If the CGW VTEP needs to route the traffic between 2 VXLAN-enabled VLANs, configure the CGW on the same VTEP for both VLANs. In other words, configure the BDI on the same VTEP for both VLANs.

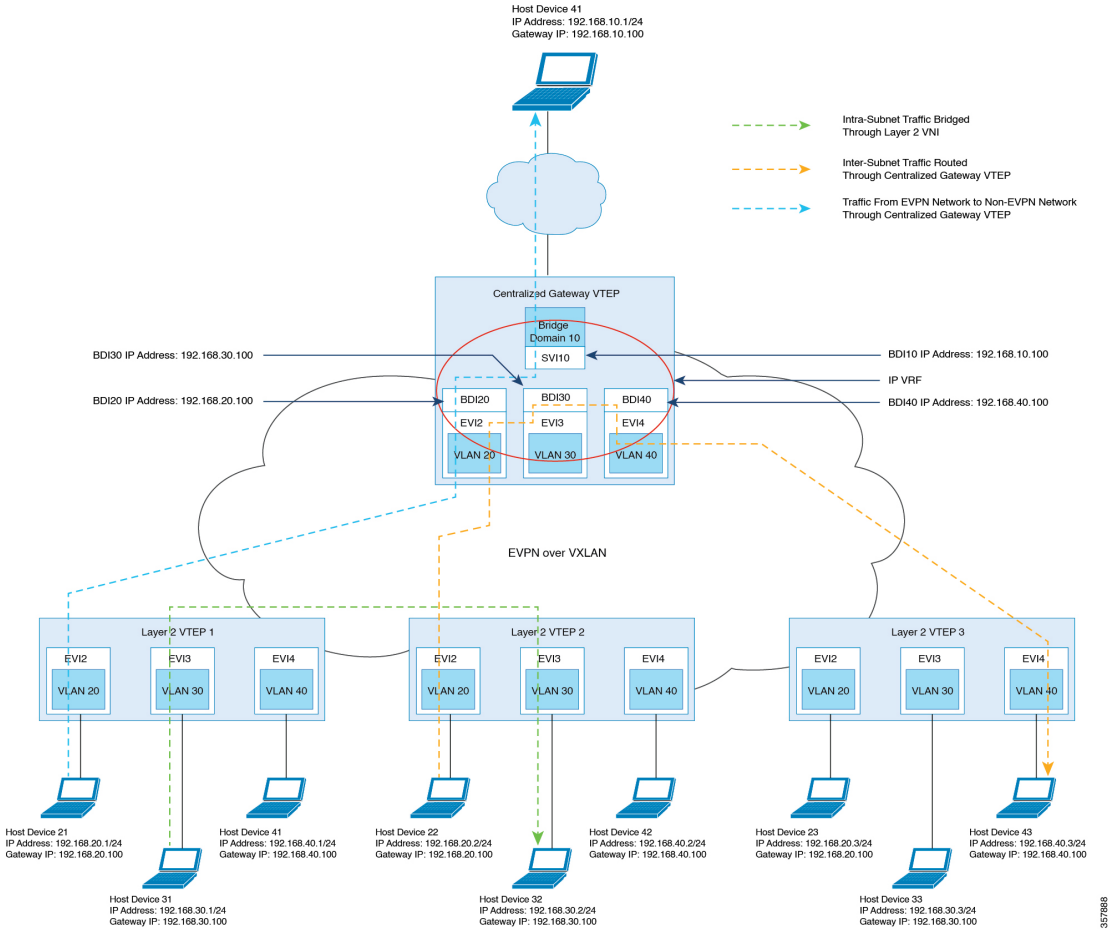
We recommend that you configure a centralized default gateway in an EVPN VXLAN network if:

- You require a boundary between the Layer 2 and Layer 3 segments at the border of the BGP EVPN VXLAN fabric.
- The intersubnet traffic is subjected to a firewall inspection or any policy on a centralized plane.

Note Toggling between DAG and CGW on a BDI in a VLAN disrupts the traffic for that VLAN.

The following image shows an EVPN VXLAN network with the centralized default gateway configured.

Figure 43: An EVPN VXLAN Network with Centralized Default Gateway



For configuration details, see Example: Configuring the EVPN VXLAN Centralized Gateway, on page 1093.

Information About EVPN VXLAN Integrated Routing and Bridging

EVPN VXLAN integrated routing and bridging (IRB) allows the VTEPs or leaf switches in an EVPN VXLAN network to perform both bridging and routing. IRB allows the VTEPs to forward both Layer 2 or bridged traffic and Layer 3 or routed traffic. A VTEP performs bridging when it forwards traffic to the same subnet. Similarly, a VTEP performs routing when it forwards traffic to a different subnet. The VTEPs in the network forward traffic to each other through the VXLAN gateways. BGP EVPN VXLAN implements IRB using symmetric IRB.

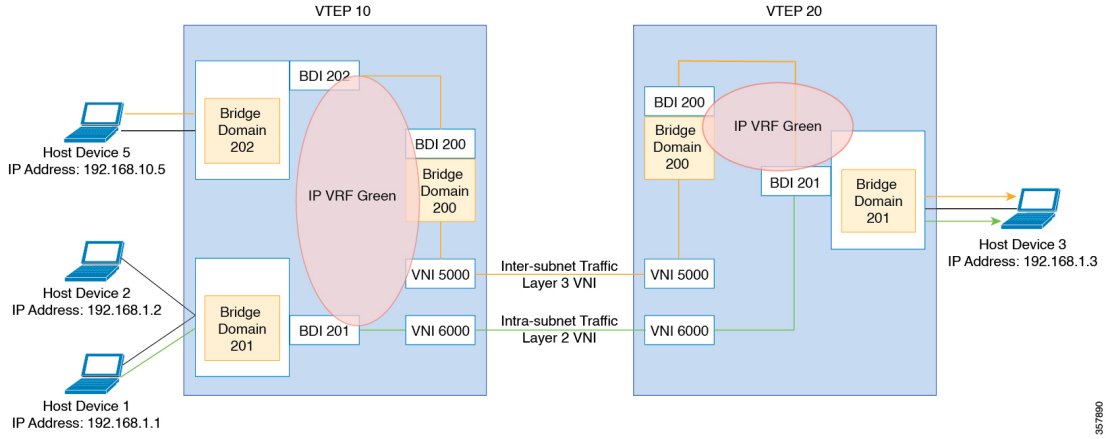
Symmetric IRB

In symmetric IRB, both the ingress and egress VTEPs perform both bridging and routing. A packet first moves through a MAC VRF, followed by an IP VRF on the NVE of the ingress VTEP. It then moves through an IP VRF followed by a MAC VRF on the NVE of the egress VTEP. The NVEs of ingress and egress VTEPs equally share all the packet processing associated with intersubnet forwarding semantics.

In symmetric IRB, you are required to define only the VNIs of locally attached endpoints in the ingress and egress VTEPs. Symmetric IRB offers better scalability in terms of the number of VNIs that a BGP EVPN VXLAN fabric supports.

The following figure shows the implementation of symmetric IRB and the movement of traffic in an EVPN VXLAN network:

Figure 44: EVPN VXLAN Integrated Routing and Bridging



For configuration details, see Example: Configuring EVPN VXLAN Integrated Routing and Bridging, on page 1097.

Default Gateway MAC Address Assignment

When leaf switches import gateway addresses, it can result in a conflict if the BDI of a leaf switch has the same IP address and MAC address as the imported addresses. To avoid this conflict, the BDI MAC-IP routes are tagged with the Default Gateway Extended Community attribute. The attribute helps the receiving leaf switches to distinguish the MAC-IP routes of the BDIs from the MAC-IP routes of the host devices. When a leaf switch receives a route tagged with the Default Gateway Extended Community attribute, it results in one of the following scenarios:

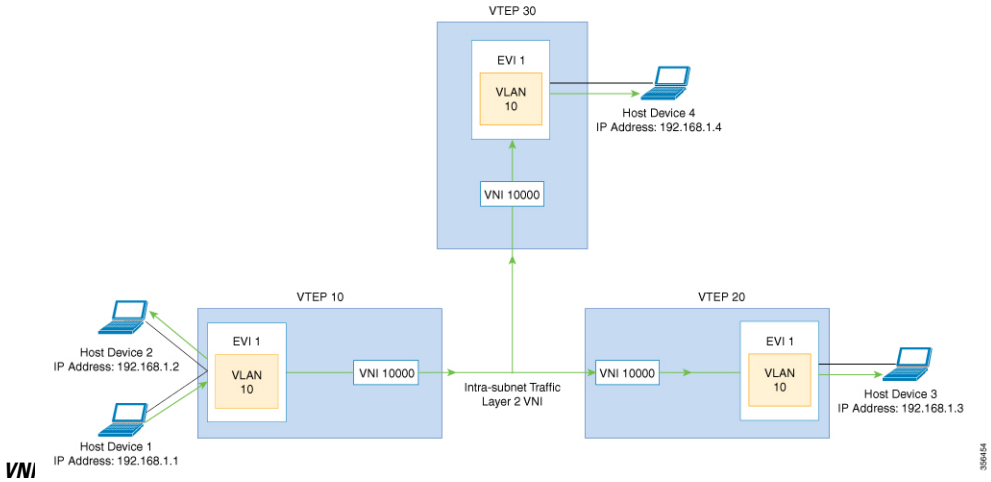
- If the leaf switch does not have a local BDI for the same MAC VRF, it installs the route only as a remote MAC route. The leaf switch implements the centralized gateway functionality in this scenario.
- If the leaf switch has a local BDI with a matching IP address but different MAC address, it installs the MAC route as a route that points to the local BDI. The leaf switch implements MAC aliasing for distributed anycast gateway in this scenario.
- If the leaf switch has an BDI with no matching IP address, it invalidates the MAC-IP route and issues an error. See RFC4732 for more details about the error.

Broadcast, Unknown Unicast, and Multicast Traffic

Multidestination Layer 2 traffic in a VXLAN network is typically referred to as broadcast, unknown unicast, and multicast (BUM) traffic. In a BGP EVPN VXLAN fabric, the underlay network forwards the BUM traffic to all the endpoints connected to a common Layer 2 broadcast domain in the VXLAN overlay.

The following image shows the flow of BUM traffic through a Layer 2 VNI. The network forwards BUM traffic from host device 1 to all the VTEPs which then send the traffic to all the host devices in the same subnet.

Figure 45: BUM Traffic through Layer 2



Ingress Replication

Ingress replication, or headend replication, is a unicast approach to handle multidestination Layer 2 overlay BUM traffic. Ingress replication involves an ingress device replicating every incoming BUM packet and sending them as a separate unicast to the remote egress devices. Ingress replication happens through EVPN route type 3, also called inclusive multicast ethernet tag (IMET) route. BGP EVPN ingress replication uses IMET route for auto discovery of remote peers in order to set up the BUM tunnels over VXLAN. Using ingress replication to handle BUM traffic can result in scaling issues because an ingress device needs to replicate the BUM traffic as many times as there are VTEPs associated with the Layer 2 VNI.

Ingress Replication Operation

IMET routes carry the remote or egress VNIs advertised from the remote peers, which can be different from the local VNI. The network creates a VXLAN tunnel adjacency when an ingress device receives IMET ingress replication routes from remote NVE peers. The tunnel adjacency is a midchain adjacency that contains IP or UDP encapsulation for the VXLAN tunnel. If there is more than one VNI along the tunnel, multiple VNIs share the tunnel. Ingress replication on EVPN can have multiple unicast tunnel adjacencies and different egress VNIs for each remote peer.

The network builds a flooded replication list with the routes advertised by each VTEP. The dynamic replication list stores all the remote destination peers discovered on a BGP IMET route in the same Layer 2 VNI. The replication list gets updated every time you configure the Layer 2 VNI at a remote peer. The network removes the tunnel adjacency and VXLAN encapsulation from the replication list every time a remote NVE peer withdraws the IMET ingress replication route. The network deletes the tunnel adjacency when no NVE peer is using it.

Any BUM traffic that reaches the ingress device gets replicated after the replication list is built. The ingress device forwards the replicated traffic throughout the network to all the remote peers in the same VNI.

Underlay Multicast

In underlay multicast, the underlay network replicates the traffic through a multicast group in PIM sparse mode. Forwarding BUM traffic using underlay multicast requires the configuration of IP multicast in the underlay network. A single copy of the BUM traffic moves from the ingress or source VTEP towards the underlay transport network. The network forwards this copy along the multicast tree so that it reaches all egress or destination VTEPs participating in the given multicast group. Various branch points in the network replicate the copy as it travels along the multicast tree. The branch points replicate the copy only if the receivers are part of the multicast group associated with the VNI.

BUM traffic forwarding through underlay multicast is achieved by mapping a Layer 2 VNI to the multicast group. This mapping must be configured on all the VTEPs associated with the Layer 2 VNI. When a VTEP joins the multicast group, it receives all the traffic that is forwarded on that group. If the VTEP receives traffic in a VNI that is not associated with it, it simply drops the traffic. This approach maintains a single link within the network, thus providing an efficient way to forward BUM traffic.

Flooding Suppression

EVPN allows the distribution of the binding between IPv4 or IPv6 addresses and MAC addresses among the VTEPs of the network. It distributes the MAC-IP binding among all the VTEPs that participate in the EVPN instance associated with the MAC-IP routes. The MAC address associated with the IPv4 or IPv6 addresses is locally known even though it is learned from a remote VTEP. Locally connected endpoints send an Address Resolution Protocol (ARP) or an IPv6 neighbor discovery request when they look for a remote endpoint. The MAC-IP binding distribution allows a VTEP to perform a lookup in the local cache when it receives an ARP or an IPv6 neighbor discovery request. If the MAC-IP address information for the remote end point is available, the VTEP uses this information to avoid flooding the ARP request or IPv6 neighbor discovery request. If the MAC or IP address information for the remote end point is not available, the request floods throughout the fabric.

Flooding suppression avoids the flooding of ARP and IPv6 neighbor discovery packets over the EVPN VXLAN network. It suppresses the flooding to both the local and remote host or access devices. The network suppresses flooding by implementing an ARP or neighbor discovery relay. This is achieved by using the known MAC address for the specified IPv4 or IPv6 address to convert broadcast and multicast requests to unicast requests. Flooding suppression is enabled by default on an EVPN-enabled VLAN. An EVPN VXLAN network suppresses the flooding for the following types of traffic.

ARP Flooding Suppression

VTEPs send ARP requests as broadcast packets. ARP requests represent a large percentage of Layer 2 broadcast traffic. Flooding suppression converts them to unicast packets and reduces the network flood.

Note An ARP packet will not be generated from a BD-VIF interface or BDI interface if MAC and IP binding is found in EVPN database on the source (ingress) VTEP.

To avoid sending an ARP and neighbor discovery request, you must apply the ARP and neighbor discovery entries on the BDI or BD-VIF associated VRFs based on the remotely learned RT-2 routes or local learned MAC or IP bindings. It helps to reduce the overall traffic and system load caused by broadcast ARP packets.

When an ARP originates from a BD-VIF or BDI interface, an ARP entry is installed directly if a MAC or IP binding is available for the target IP address in the EVPN database, without even sending a unicast ARP packet.

This behavior only limit to L2-EVPN configured with BD-VIF interface.

IPv6 Neighbor Discovery Flooding Suppression

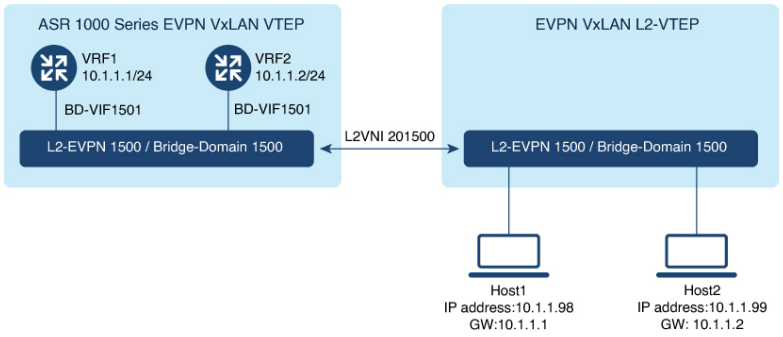
The IPv6 neighbor discovery process enables the discovery of a neighbor and helps the peers to determine each other's link-layer addresses. It also verifies the reachability of a neighbor and tracks the neighboring routers. IPv6 neighbor discovery uses Internet Control Message Protocol (ICMP) messages and solicited-node multicast addresses to achieve these functions.

Flooding suppression suppresses all multicast neighbor solicitation packets among Internet Control Message Protocol version 6 (ICMPv6) packets.

Bridge Domain VIF Support on Layer 2 EVPN

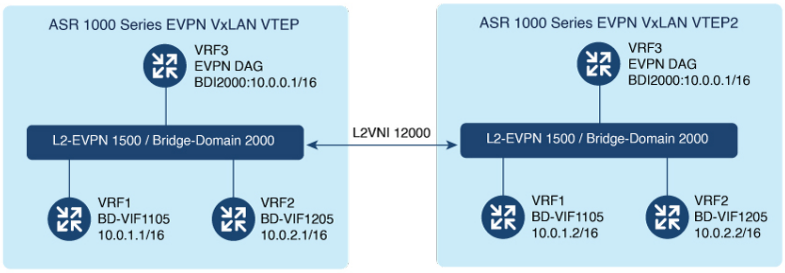
The Layer 2 EVPN only supports BDI interface that is attached to a EVPN Layer 2 network as an interface to a routing domain. The BDI servers as a centralized gateway or distributed anycast gateway in Symmetric IRB model.

Figure 46: EVPN VxLAN on Layer 2 VTEP



In some scenarios, one or more bridge domain-VIF (BD-VIF) interfaces are attached to a single EVPN Layer 2 network. Also, a BD-VIF interface is recognized by the Layer 2 EVPN network as a regular routing interface. This interface can be used as a Unicast Centralized Gateway for all, or a portion of routing-bound traffic. If you configure multiple BD-VIF interface, each bridge domain-VIF must belong to different routing domain (VRF), and should have a unique gateway IP address across the same Layer 2 EVPN network. In this scenario, hosts of the Layer 2 EVPN network can be configured to use different BD-VIF interface as a gateway.

Figure 47: EVPN VxLAN on Layer 2 VTEP-2



When a BDI interface and multiple BD-VIF interfaces co-exist within one Layer 2 EVPN network, the BDI interface must be configured as IRB interface. The other BD-VIF interfaces are treated as interfaces towards other routing domains, or gateways for VM-bound traffic.

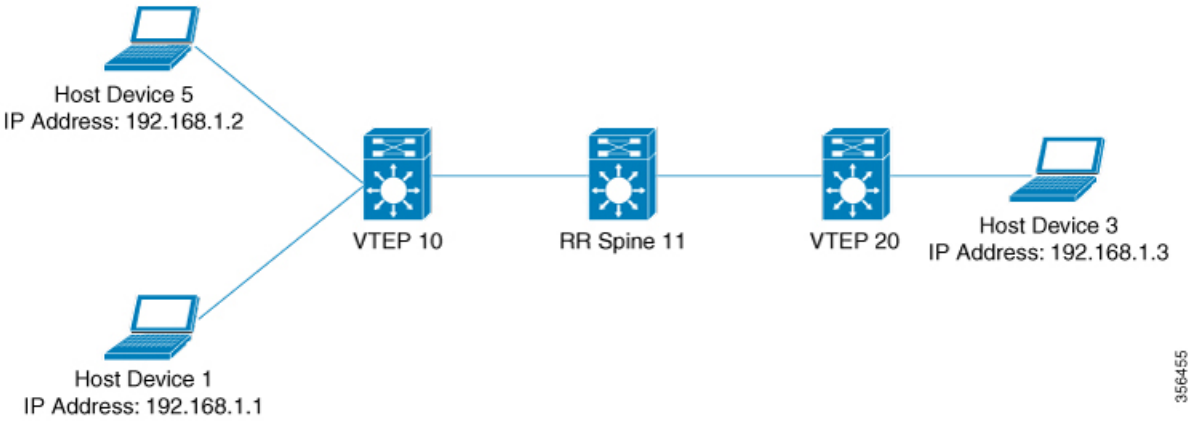
The IP address and MAC-IP binding of a BD-VIF interface is learned and advertised as regular host RT2 route, without carrying Default-Gateway Extended Community attribute.

MAC and IP Addressing Learning from a Static ARP Alias Entry

With the new functionalities, EVPN VxLAN can learn a EVPN MAC/IP binding from a static ARP alias entries immediately after the ARP alias is configured. After learning the MAC/IP binding, a EVPN route type 2 is advertised across the EVPN network. For routing purpose, the route type 2 is imported to IP VRF in remote devices as a host IP route for the IP address. A packet bound to this IP address is forwarded over Layer 3 VNI to IP VRF in the destination device.The feature enables the use of the same gateway MAC address as the RT-2 route that is advertised for BD-VIF interface MAC/IP address across all the EVPN VXLAN network.

How to Configure EVPN VXLAN Layer 2 Overlay Network

The following figure shows a sample topology of an EVPN VXLAN Network. Host device 1 and host device 3 are part of the same subnet. The network forwards BUM traffic from host device 1 to host device 3 using a Layer 2 VNI through either underlay multicast or ingress replication methods.



Note In a two-VTEP topology, a spine switch is not mandatory. For information about configuration of spine switches in an EVPN VXLAN network, see Configuring Spine Switches in a BGP EVPN VXLAN Fabric module.

Perform the following set of procedures to configure an EVPN VXLAN Layer 2 overlay network:

1. Configure BGP with EVPN address family on the VTEPs.
2. Configure Layer 2 VPN EVPN on the VTEPs.
3. Configure an EVPN instance in the VLAN on the VTEPs.
4. Configure the access-facing interface in the VLAN on the VTEPs.
5. Configure the loopback interface on the VTEPs.
6. Configure the network virtualization endpoint (NVE) interface on the VTEPs.

Configuring BGP with EVPN Address Family on a VTEP

To configure BGP with EVPN address family on the VTEPs and with a spine switch as the neighbor, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *number*
5. **neighbor** {*ip-address* | *group-name*} **update-source** *interface*
6. **address-family l2vpn evpn**
7. **neighbor** *ip-address* **activate**
8. **neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**]
9. **exit-address-family**
10. **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.

	Command or Action	Purpose
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 1`	Enables a BGP routing process, assigns it an autonomous system number, and enters router configuration mode.
Step 4	**neighbor** *ip-address* **remote-as** *number* **Example:** `Device(config-router)# neighbor 11.11.11.11 remote-as 1`	Defines multiprotocol BGP neighbors. Under each neighbor, define the Layer 2 Virtual Private Network (L2VPN) EVPN configuration. Use the IP address of the spine switch as the neighbor IP address.
Step 5	**neighbor** {*ip-address* | *group-name*} **update-source** *interface* **Example:** `Device(config-router)# neighbor 11.11.11.11 update-source Loopback0`	Configures update source. Update source can be configured per neighbor or per peer group. Use the IP address of the spine switch as the neighbor IP address.
Step 6	**address-family l2vpn evpn** **Example:** `Device(config-router)# address-family l2vpn evpn`	Specifies the L2VPN address family and enters address family configuration mode.
Step 7	**neighbor** *ip-address* **activate** **Example:** `Device(config-router-af)# neighbor 11.11.11.11 activate`	Enables the exchange information from a BGP neighbor. Use the IP address of the spine switch as the neighbor IP address.
Step 8	**neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Device(config-router-af)# neighbor 11.11.11.11 send-community both`	Specifies the communities attribute sent to a BGP neighbor. Use the IP address of the spine switch as the neighbor IP address.
Step 9	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode and returns to router configuration mode.
Step 10	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.

Configuring Layer 2 VPN EVPN on a VTEP

To configure the L2VPN EVPN parameters on a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2vpn evpn**
4. **encapsulation vxlan**
5. **replication-type** {**ingress** | **static**}
6. **exit**
7. **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	**l2vpn evpn** **Example:** `Device(config)# l2vpn evpn`	Enters EVPN configuration mode.
Step 4	**encapsulation vxlan** **Example:** `Device(config-evpn)# encapsulation vxlan`	(Optional) Defines the encapsulation format as VXLAN. The encapsulation is VXLAN by default. .
Step 5	**replication-type** {**ingress**	**static**} **Example:** `Device(config-evpn)# replication-type ingress`	Sets the replication type for the EVPN instance. **Note** Configure the L2VPN EVPN replication type as static, if multicast is enabled in the underlay network for EVPN BUM traffic. When the L2VPN EVPN replication type is configured as static, the Inclusive Multicast Ethernet Tag (IMET) route is not advertised, and forwarding of BUM traffic relies on underlay multicast being configured on each VTEP.
Step 6	**exit** **Example:** `Device(config-evpn)# exit`	Exits EVPN configuration mode and enters global configuration mode.
Step 7	**end** **Example:** `Device(config-evpn)# end`	Returns to privileged EXEC mode.

Configuring an EVPN Instance in Bridge Domain on a VTEP

To configure an EVPN instance on a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **member interface-name service-instance** *number*
5. **member evpn-instance** *evpn-instance-id* **vni** *l2-vni-number*
6. **exit**
7. **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	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 123`	Configures the bridge domain ID. • bridge-id: Bridge domain number. The bridge domain number varies depending on the platform. For Cisco ASR 1000 Series, the valid range is from 1 to 16000. For Cisco Catalyst 8000V Edge platform, the valid range is from 1 to 8192.
Step 4	**member interface-name service-instance** *number* **Example:** `Device(config-bdomain)# member GigabitEthernet1/3/1 service-instance 1000`	Configures the interface for the bridge domain.
Step 5	**member evpn-instance** *evpn-instance-id* **vni** *l2-vni-number* **Example:** `Device(config-bdomain)# member evpn-instance 23 vni 20123`	Adds EVPN instance as a member of the bridge domain configuration. The VNI here is used as an L2VNI.
Step 6	**exit** **Example:** `Device(config-evpn-evi)# exit`	Exits EVPN configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-evpn)# end`	Returns to privileged EXEC mode.

Configuring the NVE Interface on a VTEP

To add a VNI member to the NVE interface of a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface nve** *nve-interface-id*
4. **host-reachability protocol bgp**
5. **source-interface** *loopback-interface-id*
6. **member vni** *layer2-vni-id* {**ingress-replication** | **mcast-group**}<*multicast group-address*>}
7. **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 nve** *nve-interface-id* **Example:** `Device(config)# interface nve 1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 4	**host-reachability protocol bgp** **Example:** `Device(config-if)# host-reachability protocol bgp`	Configures BGP as the host-reachability protocol on the interface. **Note** You must configure the host-reachability protocol on the interface. If you do not execute this step, the VXLAN tunnel defaults to static VXLAN tunnel, which is currently not supported on the device.
Step 5	**source-interface** *loopback-interface-id* **Example:** `Device(config-if)# source-interface loopback0`	Sets the IP address of the specified loopback interface as the source IP address.

	Command or Action	Purpose
Step 6	**member vni** *layer2-vni-id* {**ingress-replication** | **mcast-group**}<*multicast group-address*>} **Example:** `Device(config-if)# member vni 39000 ingress-replication`	Associates the Layer 2 VNI member with the NVE. The specified replication type must match the replication type that is configured globally, or for the specific EVPN instance. Use the **ingress-replication** keyword for ingress replication. Use mcast-group followed by a multicast group address keywords for static multicast replication.
Step 7	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

How to Configure EVPN VXLAN Layer 2 and Layer 3 Overlay Network

The following sections provide detailed information about the various tasks that must be performed to configure an EVPN VXLAN Layer 2 and Layer 3 overlay network.

Configuring BGP on a VTEP with EVPN Address Family

To configure BGP on a VTEP with EVPN address family and with spine switch as the neighbor, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *number*
5. **neighbor** {*ip-address* | *group-name*}**update-source** *interface*
6. **address-family l2vpn evpn**
7. **neighbor** *ip-address* **activate**
8. **neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**]
9. **exit-address-family**
10. **address-family ipv4** [**mdt**] {**multicast** | **unicast**} {**vrf** *vrf name*}
11. **advertise l2vpn evpn**
12. **exit-address-family**
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router bgp** *autonomous-system-number* **Example:** `Device(config)# router bgp 1`	Enables a BGP routing process, assigns it an autonomous system number, and enters router configuration mode.
Step 4	**neighbor** *ip-address* **remote-as** *number* **Example:** `Device(config-router)# neighbor 11.11.11.11 remote-as 1`	Defines multiprotocol BGP neighbors. Under each neighbor, define the Layer 2 Virtual Private Network (L2VPN) EVPN configuration. Use the IP address of the spine switch as the neighbor IP address.
Step 5	**neighbor** {*ip-address* | *group-name*} **update-source** *interface* **Example:** `Device(config-router)# neighbor 11.11.11.11 update-source Loopback0`	Configures update source. Update source can be configured per neighbor or per peer group. Use the IP address of the spine switch as the neighbor IP address.
Step 6	**address-family l2vpn evpn** **Example:** `Device(config-router)# address-family l2vpn evpn`	Specifies the L2VPN address family and enters address family configuration mode.
Step 7	**neighbor** *ip-address* **activate** **Example:** `Device(config-router-af)# neighbor 11.11.11.11 activate`	Enables the exchange information from a BGP neighbor. Use the IP address of the spine switch as the neighbor IP address.
Step 8	**neighbor** *ip-address* **send-community** [**both** | **extended** | **standard**] **Example:** `Device(config-router-af)# neighbor 11.11.11.11 send-community both`	Specifies the communities attribute sent to a BGP neighbor. Use the IP address of the spine switch as the neighbor IP address.
Step 9	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode and returns to router configuration mode.
Step 10	**address-family ipv4** [**mdt**] {**multicast** | **unicast**} {**vrf** *vrf name*} **Example:**	Enters address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes.

	Command or Action	Purpose
	`Device(config-router)# address-family ipv4 vrf Customer1`	
Step 11	**advertise l2vpn evpn** **Example:** `Device(config-router-af)# advertise l2vpn evpn`	Advertises the L2VPN EVPN routes to the EVPN BGP neighbor.
Step 12	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode and returns to router configuration mode.
Step 13	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.

Configuring the IP VRF on a VTEP

To add a VNI member to the NVE interface of a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf name*
4. **rd** *route-distinguisher*
5. **address-family ipv4** {**multicast** | **unicast**} {**vrf***vrf name*}
6. **route-target export** *route-target-id* **stitching**
7. **route-target import** *route-target-id* **stitching**
8. **exit-address-family**
9. **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	**vrf definition** *vrf name* **Example:**	Names the VRF and enters VRF configuration mode.

	Command or Action	Purpose
	`Device(config)# vrf definition red`	
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 1.1.1.1:1`	(Optional) Creates a VRF table by specifying a route distinguisher. Enter either an Autonomous System number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Step 5	**address-family ipv4** {**multicast** | **unicast**} {**vrf***vrf name*} **Example:** `Device(config-router)# address-family ipv4 unicast`	Enters address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes.
Step 6	**route-target export** *route-target-id* **stitching** **Example:** `Device(config-if-afi)# route-target export 100:1 stitching`	Configures exporting of routes from the VRF to the EVPN BGP NLRIs and assigns the specified route-target identifiers to the BGP EVPN nodes, links, or prefixes (NLRIs).
Step 7	**route-target import** *route-target-id* **stitching** **Example:** `Device(config-if-afi)# route-target import 100:1 stitching`	Configures importing of routes from the EVPN BGP NLRI that have the matching route-target value.
Step 8	**exit-address-family** **Example:** `Device(config-router-afi)# exit-address-family`	Exits address family configuration mode and returns to router configuration mode.
Step 9	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring Layer 2 EVPN on a VTEP

For configuring Layer 2 VPN EVPN on a VTEP, see Configuring Layer 2 VPN EVPN on a VTEP, on page 1075.

Configuring an EVPN Instance in Bridge Domain on a VTEP

For configuring an EVPN instance in bridge domain on a VTEP, see Configuring an EVPN Instance in Bridge Domain on a VTEP, on page 1077.

Configuring the Per-EVI Bridge Domain on a VTEP

To configure the Per-EVI bridge domain on a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **member evpn-instance** *evpn-instance-id* **vni** *l2-vni-number*
5. **member** *interface-name* **service-instance** *number*
6. **exit**
7. **interface** *interface-name*
8. **service instance** *number* **ethernet**
9. **encapsulation dot1q**<*first tag> [second dot1q <second tag>]*
10. **exit**

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	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 10`	Configure the bridge domain ID. The range is from 1 to 4000. • bridge-id: Bridge domain number. The valid range is from 1 to 4094.
Step 4	**member evpn-instance** *evpn-instance-id* **vni** *l2-vni-number* **Example:** `Device(config-bdomain)# member evpn-instance 1 vni 39000`	Adds EVPN instance as a member of the bridge domain configuration. The VNI here is used as a Layer 2 VNI.
Step 5	**member** *interface-name* **service-instance** *number* **Example:** `Device(config-bdomain)# member GigabitEthernet0/1/0 service-instance 10`	Configures the interface for the bridge domain.
Step 6	**exit** **Example:** `Device(onfig-bdomain)# exit`	Returns to privileged EXEC mode.
Step 7	**interface** *interface-name* **Example:** `Device(config)# interface GigabitEthernet0/1/1`	Enters interface configuration mode for the specified interface.

	Command or Action	Purpose
Step 8	**service instance** *number* **ethernet** **Example:** `Device(config-if)# service-instance 10 ethernet`	Configures an EFP (service instance) and enters service instance configuration mode. • number: EFP identifier; an integer from 1 to 4000.
Step 9	**encapsulation dot1q**<*first tag*> *[second dot1q <second tag>]* **Example:** `Device(config-if-srv)# encapsulation dot1q 10`	Configures encapsulation type for the service instance.
Step 10	**exit** **Example:** `Device(onfig-if-srv)# exit`	Returns to privileged EXEC mode.

Configuring a Bridge Domain Interface Using Anycast IP and MAC Address in All Leafs

To configure a bridge domain interface using the same IP address and Mac address in all the leafs, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface BDI** *{ interface number }*
4. **mac address** *{ mac-address }*
5. **vrf forwarding** *vrf name*
6. **ip address** *ip address mask*
7. **exit**

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 BDI** *{ interface number }* **Example:** `Device(config)# interface BDI 12`	Specifies a bridge domain interface.

	Command or Action	Purpose
Step 4	**mac address** *{ mac-address }* **Example:** `Device(config-if)# mac-address 1.1.1`	Specifies the MAC address for the bridge domain interface.
Step 5	**vrf forwarding** *vrf name* **Example:** `Device(config-if)# vrf forwarding red`	Associates the VRF with the Layer 3 interface.
Step 6	**ip address** *ip address mask* **Example:** `Device(config-if)# ip address 2.2.2.254 255.255.255.0`	Specifies either the IPv4 or IPv6 address for the bridge domain interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to privileged EXEC mode.

Configuring Bridge Domain for a Layer 3 VXLAN on a VRF

To configure a bridge domain on a vrf, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **member vni** *l3-vni-number*
5. **exit**
6. **interface BDI** *{ interface number }*
7. **vrf forwarding** *vrf name*
8. **ip address** *ip address mask*
9. **exit**

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.

	Command or Action	Purpose
Step 3	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 3`	Configure the bridge domain ID. • bridge-id: Bridge domain number. The bridge domain number depends on the platform. For Cisco ASR 1000 Series, the valid range is from 1 to 16000. For Cisco Catalyst 8000V Edge platform, the valid range is from 1 to 8192.
Step 4	**member vni** *l3-vni-number* **Example:** `Device(config-bdomain)# member vni 49000`	Associates the Layer 3 VNI member with the bridge domain configuration.
Step 5	**exit** **Example:** `Device(onfig-bdomain)# exit`	Returns to privileged EXEC mode.
Step 6	**interface BDI** *{ interface number }* **Example:** `Device(config)# interface BDI 3`	Specifies a bridge domain interface.
Step 7	**vrf forwarding** *vrf name* **Example:** `Device(config-if)# vrf forwarding red`	Associates the VRF with the Layer 3 interface.
Step 8	**ip address** *ip address mask* **Example:** `Device(config-if)# ip address 20.20.20.20 255.255.255.255`	Specifies either the IPv4 or IPv6 address for the bridge domain interface.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Returns to privileged EXEC mode.

Configuring the NVE Interface on a VTEP

To configure a VNI member to the NVE interface of a VTEP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface nve** *nve-interface-id*
4. **host-reachability protocol bgp**
5. **source-interface** *loopback-interface-id*
6. **member vni** *layer2-vni-id* {**ingress-replication**}

7. **member vni** *l3-vni-number vrf name*
8. **exit**

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 nve** *nve-interface-id* **Example:** `Device(config)# interface nve 1`	Defines the interface to be configured as a trunk, and enters interface configuration mode.
Step 4	**host-reachability protocol bgp** **Example:** `Device(config-if)# host-reachability protocol bgp`	Configures BGP as the host-reachability protocol on the interface. **Note** You must configure the host-reachability protocol on the interface. If you do not execute this step, the VXLAN tunnel defaults to static VXLAN tunnel, which is currently not supported on the device.
Step 5	**source-interface** *loopback-interface-id* **Example:** `Device(config-if)# source-interface loopback0`	Sets the IP address of the specified loopback interface as the source IP address.
Step 6	**member vni** *layer2-vni-id* {**ingress-replication**} **Example:** `Device(config-if)# member vni 5011 ingress-replication`	Associates the Layer 2 VNI member with the NVE. The specified replication type must match the replication type that is configured globally, or for the specific EVPN instance. Use the **mcast-group** keyword for static replication and the **ingress-replication** keyword for ingress replication.
Step 7	**member vni** *l3-vni-number vrf name* **Example:** `Device(config-if)# member vni 49000 vrf red`	Adds EVPN instance for the interface. The VNI here is used as a Layer 3 VNI.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Returns to privileged EXEC mode.

Configuring Underlay Multicast Group

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface nve** *nve-interface-id*
4. **source-interface** *loopback-interface-id*
5. **host-reachability protocol bgp**
6. **member vni** *layer2-vni-id* {**ingress-replication** | **mcast-group** <*mcast-group-id*> }
7. **exit**
8. **l2vpn evpn instance** *evpn-instance-number* **vlan-based**
9. **encapsulation vxlan**
10. **replication-type** {**static**}
11. **default-gateway advertise** { **enable** | **disable**}
12. **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 nve** *nve-interface-id* **Example:** `Device(config)# interface nve 1`	Defines the interface and enters interface configuration mode.
Step 4	**source-interface** *loopback-interface-id* **Example:** `Device(config-if)# source-interface loopback0`	Sets the IP address of the specified loopback interface as the source IP address.
Step 5	**host-reachability protocol bgp** **Example:** `Device(config-if)# host-reachability protocol bgp`	Configures BGP as the host-reachability protocol on the interface. **Note** You must configure the host-reachability protocol on the interface. If you do not execute this step, the VXLAN tunnel defaults to static VXLAN tunnel, which is currently not supported on the device.
Step 6	**member vni** *layer2-vni-id* {**ingress-replication**	**mcast-group** <*mcast-group-id*> }	Associates the Layer 2 VNI member with the NVE.

	Command or Action	Purpose
	Example: `Device(config-if)# member vni 3017000 mcast-group 239.1.1.1`	The specified replication type must match the replication type that is configured globally or for the specific EVPN instance. Use **mcast-group** keyword for static replication and **ingress-replication** keyword for ingress replication.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 8	**l2vpn evpn instance** *evpn-instance-number* **vlan-based** **Example:** `Device(config)# l2vpn evpn instance 1700 vlan-based`	Enters EVPN configuration mode and configures VLAN-based instance.
Step 9	**encapsulation vxlan** **Example:** `Device(config-evpn)# encapsulation vxlan`	(Optional) Defines the encapsulation format as VXLAN.The encapsulation format is VXLAN by default. .
Step 10	**replication-type** {**static**} **Example:** `Device(config-evpn)# replication-type static`	Sets the replication type for the EVPN instance. **Note** Configure the L2VPN EVPN replication type as static, if multicast is enabled in the underlay network for EVPN BUM traffic. When the L2VPN EVPN replication type is configured as static, the IMET route is not advertised and forwarding of BUM traffic relies on underlay multicast being configured on each VTEP.
Step 11	**default-gateway advertise** { **enable** | **disable**} **Example:** `Device(config-evpn))# default-gateway advertise disable`	(Optional) Enables or disables the default gateway advertisement for the EVPN instance. In case default gateway advertisement has already been globally configured, this overrides the global setting. This command is mandatory only if the same MAC address is not manually configured on all the access SVIs. To configure distributed anycast gateway in a VXLAN network using MAC aliasing, enable default gateway advertisement on all the leaf switches in the network
Step 12	**end** **Example:** `Device(config-evpn)# end`	Returns to privileged EXEC mode.

Configuring a NAT and ARP Alias

To configure the bridge domain VIF interfaces as NAT inside interface or outside interface, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface BD-VIF** *unit number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address ip address subnet mask**
6. **ip nat inside**
7. **exit**
8. **interface BD-VIF** *unit number*
9. **ip vrf forwarding** *vrf-name*
10. **ip address ip address subnet mask**
11. **ip nat outside**
12. **ipv6 address** *{ ipv6-address | prefix length }*
13. **ip nat inside source static** {*local-ip* | *global-ip*} **no alias**
14. **arp vrf** [*vrf-name*] **ip address** [**alias**]
15. **exit**

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 BD-VIF** *unit number* **Example:** `Device(config)# interface BD-VIF1101`	Enters interface configuration mode and specify the Layer 3 interface to be associated with the bridge domain VIF. The interface can be a routed port BDI.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding customer-vrf-a`	Associates the VRF with the Layer 3 interface.
Step 5	**ip address ip address subnet mask** **Example:** `Device(config-if-vrf)# ip address 192.168.101.14 255.255.255.240`	Enters the IP address for the interface.

	Command or Action	Purpose
Step 6	**ip nat inside** **Example:** `Device(config-if-vrf)# ip nat inside`	Connects the interface to the inside network, which is subject to NAT.
Step 7	**exit** **Example:** `Device(config-if-vrf)# exit`	Exits interface configuration mode, and returns the device to global configuration mode.
Step 8	**interface BD-VIF** *unit number* **Example:** `Device(config)# interface BD-VIF2101`	Enters interface configuration mode and specify the Layer 3 interface to be associated with the bridge domain VIF. The interface can be a routed port BDI.
Step 9	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding customer-vrf-a`	Associates the VRF with the Layer 3 interface.
Step 10	**ip address ip address subnet mask** **Example:** `Device(config-if-vrf)# ip address 200.168.101.14 255.255.0.0`	Enters the IP address for the interface.
Step 11	**ip nat outside** **Example:** `Device(config-if-vrf)# ip nat outside`	Connects the interface to the outside network, which is subject to NAT.
Step 12	**ipv6 address** *{ ipv6-address | prefix length }* **Example:** `Device(config-if-vrf)# ipv6 address 3001::101:14/96`	Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface.
Step 13	**ip nat inside source static** {*local-ip* | *global-ip*} **no alias** **Example:** `Device(config-if-vrf)# ip nat inside source static 192.168.101.11 200.168.101.11 vrf customer-vrf-a no alias`	Establishes static translation between an inside local address and an inside global address. **Note** Use no-alias form of the command for all Static NAT.
Step 14	**arp vrf** [*vrf-name*] **ip address** [**alias**] **Example:** `Device(config-if-vrf)# arp vrf customer-vrf-a 200.168.101.11 aabb.cc02.d0fe ARPA alias`	Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface.
Step 15	**exit** **Example:** `Device(config-if-vrf)# exit`	Exits interface configuration mode, and returns the device to global configuration mode.

Configuration Examples of VXLAN BGP EVPN

This section provides examples for configuring an EVPN VXLAN Layer 2 overlay network.

Example: Configuring BGP with EVPN Address Family

```
Device (config)# router bgp 1
Device (config-router)# neighbor 11.11.11.11 remote-as 1
Device (config-router)# neighbor 11.11.11.11 update-source Loopback0
Device (config-router)# address-family l2vpn evpn
Device (config-router-af)# neighbor 11.11.11.11 activate
Device (config-router-af)# neighbor 11.11.11.11 send-community both
Device (config-router-af)# exit-address-family
Device (config-router)# exit
```

Example:Configuring Layer 2 VPN EVPN on a VTEP

```
Device(config)# l2vpn evpn
Device(config-evpn)# encapsulation vxlan
device(config-evpn)# replication-type ingress
Device(config-evpn)# exit
```

Example: Configuring an EVPN Instance in the Bridge Domain on a VTEP

```
Device(config)# bridge-domain 123
Device(config-bdomain)# member GigabitEthernet1/3/1 service-instance 1000
Device(config-bdomain)# member evpn-instance 23 vni 20123
Device(config-evpn-evi)# exit
```

Example: Configuring the NVE Interface on a VTEP

```
Deviceconfig)# interface nve 1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# source-interface loopback0
Device(config-if)# member vni 39000 ingress-replication
Device(config-if)# exit
```

Example:Layer 2 and Layer 3 BGP Configuration

```
Device(config)# router bgp 1
Device(config-router)# neighbor 11.11.11.11 remote-as 1
Device(config-router)# neighbor 11.11.11.11 update-source Loopback0
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 11.11.11.11 activate
Device(config-router-af)# neighbor 11.11.11.11 send-community both
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf Customer1
Device(config-router-af)# advertise l2vpn evpn
Device(config-router-af)# exit-address-family
```

Example: Configuring IP VRF

```
Device(config)# vrf definition red
Device(config-vrf)# rd 1.1.1.1:1
Device(config-vrf)# address-family ipv4 unicast
Device(config-vrf-afi)# route-target export 100:1 stitching
Device(config-vrf-afi)# route-target import 100:1 stitching
```

Example: Configuring a Bridge-domain Interface using same IP and MAC address in all leafs

```
Device(config)# interface BDI 12
Device(config-if)# mac-address 0001.0001.0001
Device(config-if)# vrf forwarding red
Device(config-if)# ip address  2.2.2.254 255.255.255.0
Device(config-if)# exit
```

Example: Configuring Bridge Domain on a VRF

```
Device(config)# bridge-domain 3
Device(config-bdomain)# member vni 49000
Device(config-bdomain)# exit
Device(config)# interface BDI 3
Device(config-if)# vrf forwarding red
Device(config-if)# ip address 20.20.20.20 255.255.255.255
Device(config-if)# exit
```

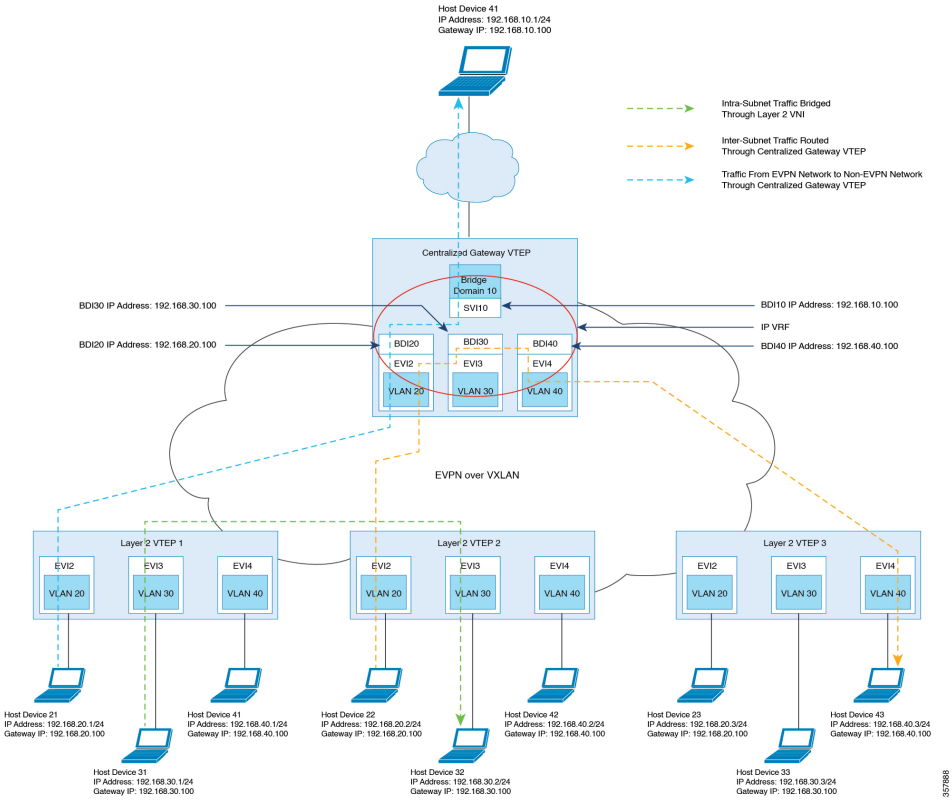
Example: Configuring the Layer 2 and Layer 3 NVE Interface on a VTEP

```
Device(config)# interface nve 1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# source-interface loopback0
Device(config-if)# member vni 39000 multicast-group 225.1.1.1
Device(config-if)# member vni 49000 vrf red
Device(config-if)# exit
```

Example: Configuring the EVPN VXLAN Centralized Gateway

This section provides an example that shows how EVPN VXLAN is configured using centralized default gateway.

Figure 48: An EVPN VXLAN Network with Centralized Default Gateway




```
VTEP1 Configuration
!
Device(config)# l2vpn evpn instance 20 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Device(config)# l2vpn evpn instance 30 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Device(config)# l2vpn evpn instance 40 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Deviceconfig)# interface nve1
Device(config-if)# member vni 400020 ingress-replication
Device(config-if)# member vni 400030 ingress-replication
Device(config-if)# member vni 400040 ingress-replication
!
Device(config)# bridge-domain 20
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 20
Device(config-bdomain)# member evpn-instance 20 vni 400020
!
Device(config)# bridge-domain 30
```

```
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 30
Device(config-bdomain)# member evpn-instance 30 vni 400030
!
Device(config)# bridge-domain 40
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 40
Device(config-bdomain)# member evpn-instance 40 vni 400040
!
VTEP2 Configuration
!
Device(config)# l2vpn evpn instance 20 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Device(config)# l2vpn evpn instance 30 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Device(config)# l2vpn evpn instance 40 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Deviceconfig)# interface nve1
Device(config-if)# member vni 500020 ingress-replication
Device(config-if)# member vni 500030 ingress-replication
Device(config-if)# member vni 500040 ingress-replication
!
Device(config)# bridge-domain 20
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 20
Device(config-bdomain)# member evpn-instance 20 vni 500020
!
Device(config)# bridge-domain 30
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 30
Device(config-bdomain)# member evpn-instance 30 vni 500030
!
Device(config)# bridge-domain 40
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 40
Device(config-bdomain)# member evpn-instance 40 vni 500040
!

VTEP3 Configuration

Device(config)# l2vpn evpn instance 20 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Device(config)# l2vpn evpn instance 30 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Device(config)# l2vpn evpn instance 40 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Deviceconfig)# interface nve1
Device(config-if)# member vni 600020 ingress-replication
Device(config-if)# member vni 600030 ingress-replication
Device(config-if)# member vni 600040 ingress-replication
```

```
!
Device(config)# bridge-domain 20
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 20
Device(config-bdomain)# member evpn-instance 20 vni 600020
!
Device(config)# bridge-domain 30
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 30
Device(config-bdomain)# member evpn-instance 30 vni 600030
!
Device(config)# bridge-domain 40
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 40
Device(config-bdomain)# member evpn-instance 40 vni 600040
!
```

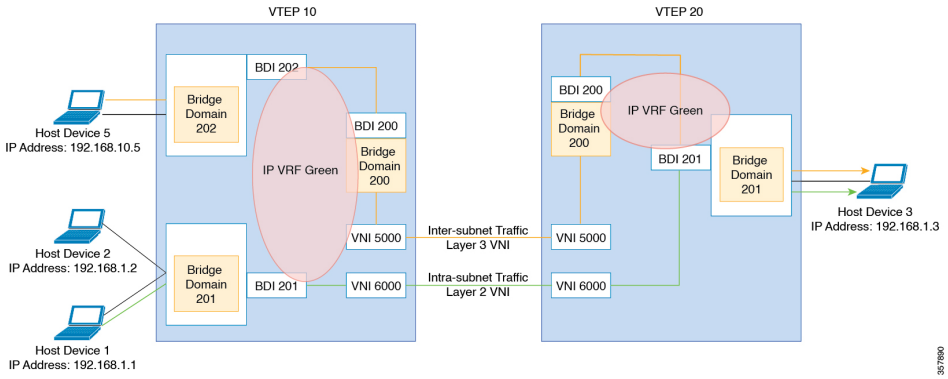
VTEP Configuration

```
!
Device(config)# l2vpn evpn instance 20 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Device(config)# l2vpn evpn instance 30 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Device(config)# l2vpn evpn instance 40 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enabl
!
Deviceconfig)# interface nve1
Device(config-if)# member vni 300020 ingress-replication
Device(config-if)# member vni 300030 ingress-replication
Device(config-if)# member vni 300040 ingress-replication
!
Device(config)# bridge-domain 20
Device(config-bdomain)# member evpn-instance 20 vni 300020
!
Device(config)# bridge-domain 30
Device(config-bdomain)# member evpn-instance 30 vni 300030
!
Device(config)# bridge-domain 40
Device(config-bdomain)# member evpn-instance 40 vni 300040
!
Device(config)# interface BDI20
Device(config-if)# vrf forwarding Green
Device(config-if)# mac-address  0020.0020.0020
Device(config-if)# ip address 192.168.20.100 255.255.255.0
Device(config-if)# ipv6 address 2000::1/96
!
Device(config)# interface BDI30
Device(config-if)# vrf forwarding Green
Device(config-if)# mac-address 0030.0030.0030
Device(config-if)# ip address 192.168.30.100 255.255.255.0
Device(config-if)# ipv6 address 3000::1/96
!
Device(config)# interface BDI40
Device(config-if)# vrf forwarding Green
Device(config-if)# mac-address 0040.0040.0040
Device(config-if)# ip address 192.168.40.100 255.255.255.0
Device(config-if)# ipv6 address 4000::1/96
!
```

Example: Configuring EVPN VXLAN Integrated Routing and Bridging

This section provides an example that shows how EVPN VXLAN IRB is configured.

Figure 49: EVPN VXLAN Symmetric IRB Topology




```
Device(config)# l2vpn evpn instance 201 vlan-based
Device (config-evpn-evi)# encapsulation vxlan
Device config-evpn-evi)# replication-type ingress
Device config-evpn-evi)# default-gateway advertise enable
!
Deviceconfig)# interface nve 1
Device(config-if)# member vni 6000 ingress-replication
Device(config-if)# member vni 5000   vrf Green
!
Device(config)# bridge-domain 200
Device(config-bdomain)# member vni 5000
!
Device(config)# bridge-domain 201
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 201
Device(config-bdomain)# member evpn-instance 201 vni 6000
!
Device(config)# bridge-domain 202
Device(config-bdomain)# member GigabitEthernet0/0/1 service-instance 201
!

Device(config)# interface BDI200
Device(config-if)# mac-address 0033.bdf8.0100
Device(config-if)# vrf forwarding Green
Device(config-if)# ip address 10.246.103.100 255.255.255.0
!
Device(config)# interface BDI202
Device(config-if)# mac-address 0022.bdf8.0202
Device(config-if)# vrf forwarding ZoneB
Device(config-if)# ip address 192.168.10.1 255.255.255.0
Device(config-if)# ipv6 address 202::1/120
!
Device(config)# interface BDI201
Device(config-if)# mac-address 0022.bdf8.0200
Device(config-if)# vrf forwarding ZoneB
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# ipv6 address 200::1/120

!
```

Example: Configuring Uderlay Multicast Group

```
Device# configure terminal
Device(config)# interface nve 1
Device(config-if)# source-interface loopback0
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 3017000 mcast-group 239.1.1.1
Device(config-if)# exit
Device(config)# l2vpn evpn instance 1700 vlan-based
Device(config-evpn)# encapsulation vxlan
Device(config-evpn)# replication-type static
Device(config-evpn))# default-gateway advertise disable
Device(config-evpn)# end
```

Example: Configuring a Bridge Domain VIF Interface as a Pseudo-port

```
Device# configure terminal
Device(config)# bridge-domain 102
Device(config-bdomain)# member evpn-instance 2 vni 20102
Device(config-evpn)# member BD-VIF1102
Device(config-evpn)# member BD-VIF1103
Device(config-evpn)# exit
```

Example: Configuring a NAT and ARP Alias

```
Device(config)# interface BD-VIF1101
Device(config-if)# vrf forwarding customer-vrf-a
Device(config-vrf)# ip address 192.168.101.14 255.255.255.240
Device(config-vrf)# ip nat inside
Device(config-router-vrf)# ipv6 address 2001:101::14/124
Device(config-router-af)# exit
```

NAT Outside BD-VIF

```
Device(config)# interface BD-VIF2101
Device(config-if)# vrf forwarding customer-vrf-a
Device(config-vrf)# ip address 200.168.101.14 255.255.0.
Device(config-vrf)# ip nat outside
Device(config-router-vrf)# ipv6 address 3001::101:14/96
Device(config-router-vrf)# ip nat inside source static 192.168.101.11 200.168.101.11 vrf
customer-vrf-a
Device(config-router-vrf)# arp vrf customer-vrf-a 200.168.101.11 aabb.cc02.d0fe ARPA alias
Device(config-router-af)# exit
```

Additional References for EVPN VXLAN Layer 2

MIBs

MIB	MIBs Link
• CISCO-VXLAN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

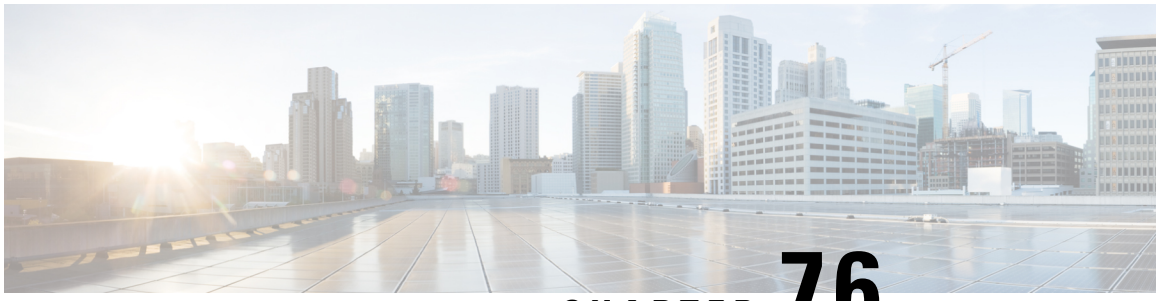
Feature Information for Layer 2 EVPN VXLAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 97: Feature Information for EVPN VxLAN L2

Feature Name	Releases	Feature Information
EVPN VXLAN L2	Cisco IOS XE Cupertino 17.10.1	BGP EVPN VXLAN is a campus network solution for Cisco routers running Cisco IOS XE software. This solution is a result of proposed IETF standards and Internet drafts submitted by the BGP Enabled ServicesS (bess) workgroup. It is designed to provide a unified overlay network solution and also address the challenges and drawbacks of existing technologies. BGP VXLAN EVPN are applicable only on Cisco ASR 1000 Series, Cisco Catalyst 8500 Edge Series platforms, and Cisco Catalyst 8000V Edge platform.
EVPN VXLAN L2	Cisco IOS XE Dublin 17.11.1a	Multi-destination Layer 2 broadcast, unknown unicast, and multicast (BUM) traffic in an EVPN VXLAN network is replicated through a multicast group in the underlay network and forwarded to all the endpoints of the network. With the new functionalities, EVPN VxLAN can learn a EVPN MAC/IP binding from a static ARP alias entries immediately after the ARP alias is configured. After learning the MAC/IP binding, a EVPN route type 2 is advertised across the EVPN network.



CHAPTER 76

VxLAN Static Routing

VxLAN static routing provides a method for connecting multiple servers in a data center to an enterprise edge router. The method:

- Creates one-to-many static routes between the servers and enterprise edge router
- Automatically generates a point-to-multipoint (P2MP) VxLAN tunnels on the static routes on demand

Feature Information for VxLAN Static Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 98: Feature Information for VxLAN Static Routing

Feature Name	Releases	Feature Information
VxLAN Static Routing	Cisco IOS XE Gibraltar 16.10.1	VxLAN static routing configures P2MP underlay tunnels between the router and multiple servers, and overlay routing within those tunnels. VxLAN static routing supports GPE and dummy-L2 P2MP tunnels. The prefix supports only IPv4. The next hop supports IPv4 and IPv6. The following commands were modified or added by this feature: **vxlan route-profile** , **show vxlan route-profile all**, **show vxlan static-route**, **show vxlan static-route next-hop bind-label**.
VxLAN Static Routing	Cisco IOS XE Gibraltar 16.11.1	Added point-to-many point "ingress" tunnels from multiple servers to the router. Added ability to specify a range of numbers for naming the tunnels, such as beginning with Tunnel100 and ending with Tunnel1000. The number is incremented by 1 for each new tunnel. Added **show** commands that provide packet/byte statistics.
IPv6 Prefix for VxLAN Static Route	Cisco IOS XE Gibraltar 16.12.x	The VxLAN tunnels that operate at more than 10 gbps provide different types of encapsulations- IPv4-over-IPv4, IPv4-over-IPv6, IPv6-over-IPv4, and IPv6-over-IPv6.
VNET/VNI VRF Policing and Accounting	Cisco IOS XE Amsterdam 17.1	Added information on VNET/VNI per-vrf policing and accounting. Added the following commands: • vxlan static-route policy output • vrf vrf1 • police match any vni 1 rate

Feature Name	Releases	Feature Information
Ingress and Egress Accounting MIB	Cisco IOS XE Amsterdam 17.2	newly added per VNI/VNET per VRF ingress and engress accounting MIB allows the user to access the counts by SNMP

Prerequisites for VxLAN Static Routing

- Underlay protocol, such as OSPF or IS-IS

Notes and Limitations for VxLAN Static Routing

- Tunnels initiating using this method can encapsulate, but not decapsulate packets. The tunnel carries packets from the customer side to the cloud service side. A static tunnel carry packets sent from the cloud service to the customer side.
- You cannot modify a route profile if it is in use. It is considered to be in use if a tunnel that was created using the method described here is currently open.

Information About VxLAN Static Routing

Overview of VxLAN Static Routing

VxLAN static routing configures P2MP underlay tunnels between the router and multiple servers, and overlay routing within those tunnels. This connects multiple servers in a data center to the enterprise edge router. VxLAN static routing supports GPE and dummy-L2 P2MP tunnels.

VxLAN static routing provides a method for connecting multiple servers in a data center to an enterprise edge router. VxLAN static routing supports GPE and dummy-L2 P2MP tunnels.

This method:

- Creates one-to-many static routes between the servers and enterprise edge router
- Automatically generates VxLAN tunnels on the static routes on demand

A use case is, connecting the servers that provide cloud services to customers and the enterprise edge routers, such as a Cisco ASR 1000 Series router, that communicates with customers.

Advantages:

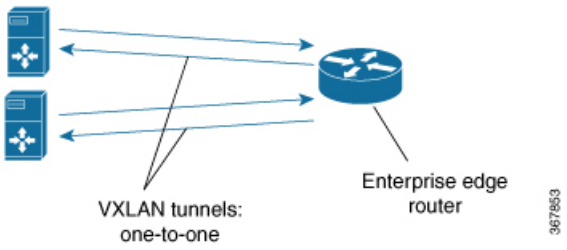
- High throughput dedicated VPN connectivity between servers and enterprise edge router
- Low latency
- Predictable performance (helps to meet service level agreements)
- High availability

-

Method

An earlier method of connecting multiple servers to a single enterprise edge router was numerous P2P connections.

Figure 50: One-to-One VxLAN Tunnels



VxLAN P2MP Tunnels provide one-to-many VxLAN tunnels in the router-to-server direction (egress), or in both the router-to-server and server-to-router (ingress) directions. The VxLAN tunnels operate at more than 10 Gbps, and can provide different types of encapsulation including IPv4-over-IPv4, IPv4-over-IPv6, IPv6-over-IPv4, and IPv6-over-IPv6.

Figure 51: One-to-Many VxLAN Tunnels, Egress Only

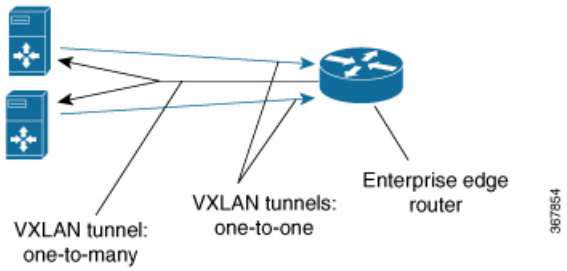
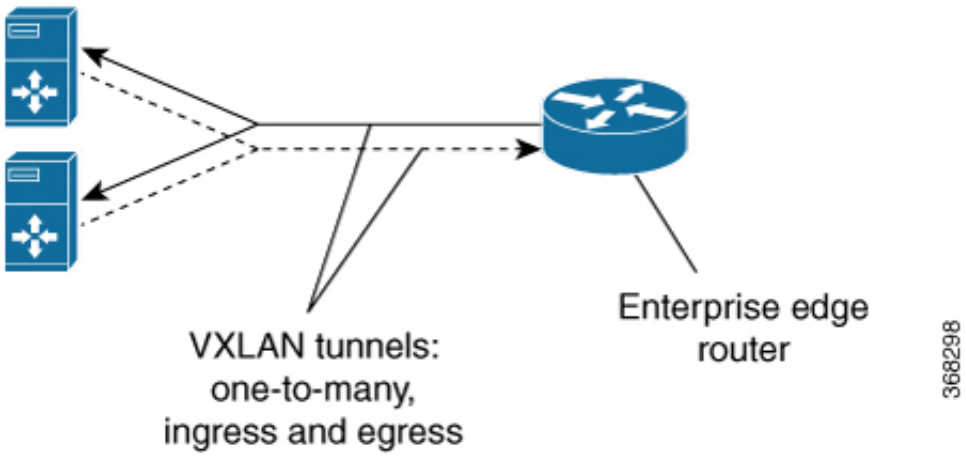


Figure 52: One-to-Many VxLAN Tunnels, Egress and Ingress



Typically, a network controller is used to manage the enterprise edge router and initiate the tunnel connections. The overall architecture for the cloud services use case is as follows:

Figure 53: Complete Architecture, Egress Only Configuration

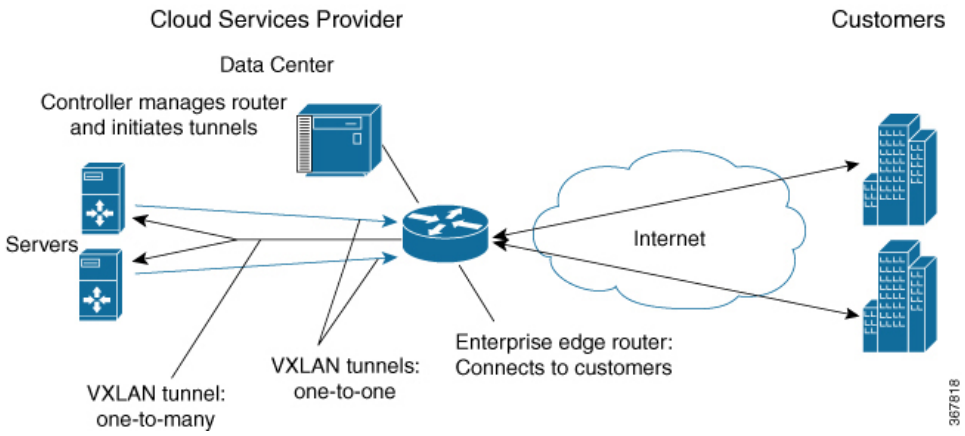
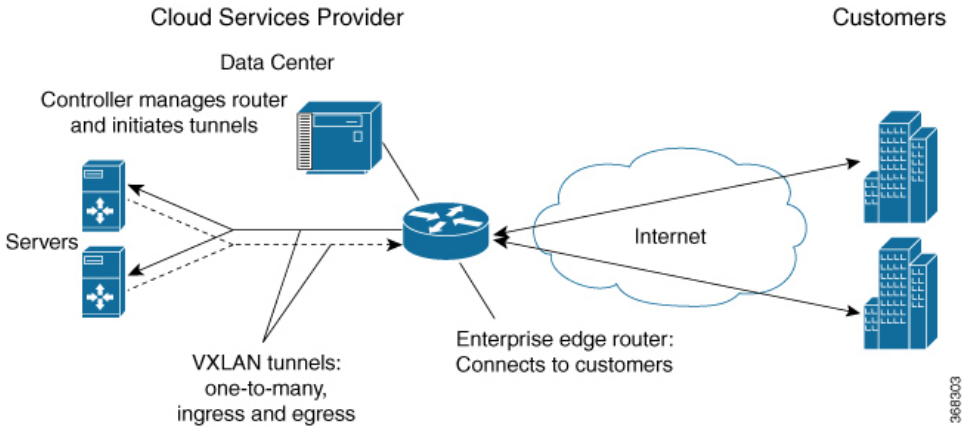


Figure 54: Complete Architecture, Egress and Ingress Configuration



How to Configure VxLAN Static Routing

Configuring VxLAN Static Routing

Perform this procedure on a router. A remote controller can initiate the tunnels.

1. Use **vxlan route-profile** to define a profile to use when creating new tunnels.
2. Use **vxlan static-route** to define multiple endpoints (servers).

Before you begin

Prerequisites: Underlay protocol, such as OSPF or IS-IS

Procedure

	Command or Action	Purpose

Step 1	**vxlan route-profile** *route-profile-name* **tunnel source interface** *interface* [**default-mac-source** *mac-address*] [**dscp** *dscp*] [**dst-port** *port*] [**tunnel mode** *mode*] [**tunnel mtu** *mtu*] [**tunnel source-port-hash** *hash*] [**tunnel source-port range** *port-range*] [**vxlan-reserved-word-1** *0x0000*] [**vxlan-reserved-word-2** *0x0000*] [**persistent**]
	Example:
	`vxlan route-profile af11`
	`dscp 10`
	`vxlan-reserved-word-1 1111`
	`vxlan-reserved-word-2 17`
	`tunnel mode vxlan-default-mac`
	`tunnel source interface Loopback0`
	`default-mac-source 0011.0011.0011`
	`persistent`
		Creates a route-profile.
		For tunnel mode, there are two options:
		• vxlan-gpe
		• vxlan-default-mac
		Note A route profile cannot be modified if it is in use. It is considered to be in use if a tunnel that was created using the method described here is currently open.

Step 2	**vxlan static-route** **Example:** `vxlan static-route`	Creates a static route for one or more end-points (servers). In the following step, add a separate vrf line for each end-point.
Step 3	**vxlan static-route auto-tunnel range** *start end* **Example:** `vxlan static-route auto-tunnel range 100 100000`	(Optional)

Step 4	**vrf** *vrf-name IPv4/IPv6-address* {*mask-format-X.X.X.X* | *mask-format-/XX*} **vni** *1-16777215 next-hop-IPv4/IPv6* **dst-mac** *MAC-Address* **route-profile** *route-profile-name* [**symmetric**] [**persistent**]
	Example:
	`vxlan static-route`
	`vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.0010 route-profile af11 persistent`
	`vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.0010 route-profile af11 persistent`
	`vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.001a route-profile af21 persistent`
	`vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.001a route-profile af21 persistent`
		Use the *route-profile-name* defined in an earlier step.
		persistent: Save the configuration line in the device NVRAM, persists even if device reboots.
		symmetric: Use the configured point-to-many-point tunnel for ingress also. Applies only to the specified vni.
		The prefix used for overlay supports only IPv4 addresses . Tthe next hop used for underlay supports IPv4 and IPv6.

Examples

Example: Point-to-many-point Tunnel for Egress

The **vxlan route-profile** defines a profile to use when creating new tunnels.

The **vrf** lines following **vxlan static-route** define multiple endpoints (servers).

```
vxlan route-profile af11
dscp 10
vxlan-reserved-word-1 1111
vxlan-reserved-word-2 17
tunnel mode vxlan-default-mac
tunnel source interface Loopback0
default-mac-source 0011.0011.0011
persistent

vxlan static-route
vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.0010 route-profile
 af11 persistent
vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.0010 route-profile
 af11 persistent
vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.001a route-profile
 af21 persistent
vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.001a route-profile
 af21 persistent
```

Example: Symmetric Point-to-many-point Tunnels for Egress and Ingress

The **vxlan route-profile** line defines a profile to use when creating new tunnels.

The **vxlan static-route auto-tunnel range** line sets the range for numbering of tunnel names.

The **vrf** lines following **vxlan static-route** define multiple endpoints (servers), creating symmetric point-to-many-point tunnels in both directions between the servers and the router.

```
vxlan route-profile af11
dscp 10
vxlan-reserved-word-1 1111
vxlan-reserved-word-2 17
tunnel mode vxlan-default-mac
tunnel source interface Loopback0
default-mac-source 0011.0011.0011
persistent

vxlan static-route auto-tunnel range 100 100000

vxlan static-route
vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.0010 route-profile
 af11 symmetric persistent
vrf host1_1_1 100.0.10.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.0010 route-profile
 af11 symmetric persistent
vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 11.11.11.11 dst-mac 0011.0000.001a route-profile
 af21 symmetric persistent
vrf host1_1_1 100.0.20.0 255.255.255.0 vni 1 1111::1111 dst-mac 0011.0000.001a route-profile
 af21 symmetric persistent
```

Viewing VxLAN Static Routing Status

SUMMARY STEPS

1. **show vxlan route-profile all**
2. **show vxlan static-route** { all | summary | vrf *vrf-name* }
3. **show vxlan route-profile name** *profile-name* **auto-tunnel**
4. **show vxlan static-route next-hop bind-label** *tunnel-id*
5. **show vxlan static-route statistics vrf test all detail**
6. **show vxlan static-route statistics vni** *vni* **detail**

DETAILED STEPS

Step 1 **show vxlan route-profile all**

Displays all route-profile configurations.

Step 2 **show vxlan static-route** { all | summary | vrf *vrf-name* }

Displays VxLAN static route configurations.

Example:

Example of summary output:

```
Device# show vxlan static-route summary
vxlan static-route summary:
prefix count: 6
persistent prefix count: 5
route-profile count: 2
vxlan next-hop count: 8
vxlan auto-tunnel count: 4
vxlan auto-tunnel range: [200000, 300000]
default dst mac: 0000.5e00.5214
```

Example:

Example of detailed output for a specific VRF:

```
Device# show vxlan static-route vrf test 2.2.2.8/32 detailed
vrf test2 2.2.2.8/32 vni 8 3.3.3.2 route-profile test2, binding_label: 0x2000008, connection_id: 8
vrf test2 2.2.2.8/32 vni 8 3.3.3.3 route-profile test2, binding_label: 0x2000006, connection_id: 6
vrf test2 2.2.2.8/32 vni 8 3.3.3.3 dst-mac 1212.1212.1212 route-profile test2, binding_label: 0x2000007,
 connection_id: 7
```

Step 3 **show vxlan route-profile name** *profile-name* **auto-tunnel**

Displays any active tunnels that have been generated automatically using the specified route profile. Tunnel IDs are generated automatically, numbered consecutively within a preset range.

Note If there are active tunnels using a route profile, the route profile cannot be altered.

Example:

```
Device# show vxlan route-profile name test auto-tunnel
Vxlan Route Profile test:
  IPv4 auto tunnel: Tunnel200000
  IPv6 auto tunnel: Tunnel200001
```

Step 4 **show vxlan static-route next-hop bind-label** *tunnel-id*

Displays the details of the next-hop (server address) for a specific IP static route which is identified by a hexadecimal bind-label. Use **show ip route** to display the routes that have been configured, and the bind-labels for each route.

Example:

This example uses **show ip route** to display the routes on the route_symmetric VRF. It displays details for the route with a bind-label of 0x2000002 (in the output highlighted the binding label 0x2000002).

```
Device# show ip route vrf route_symmetric
Routing Table: scale_route_symmetric
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is not set
      111.0.0.0/32 is subnetted, 91355 subnets
S        111.0.33.198 [1/0] via binding label: 0x2000002

Device# show vxlan static-route next-hop bind-label 0x2000002
vxlan static route next hop:
vni: 2
address: 20.1.1.1
auto interface: Tunnel0
route profile: test
connection-id: 2
bind-label: 0x2000002
refer count: 1
```

Step 5 **show vxlan static-route statistics vrf test all detail**

Displays the packets and bytes sent over each VRF. This info is useful for accounting purposes.

Note Enter the **ip cef accounting per-prefix** command before using this **show** command.

Example:

```
Device#ip cef accounting per-prefix
Device#show vxlan static-route statistics vrf test all detail
Vrf                  Prefix               Tx-Pkts      Tx-Bytes
test              100.0.30.0/24        0            0
test              100.0.30.2/32        3317         4630532
test              100.0.30.3/32        3317         4630532
------------------------------------------------------------
                                       6634         9261064
```

Step 6 **show vxlan static-route statistics vni** *vni* **detail**

Displays the packets and bytes for a specific VNI. This info is useful for accounting purposes.

Example:

```
Device#show vxlan static-route statistics vni 100 detail
Vni    Next-hop         Intf            Route-profile   Pkts    Bytes
100    11.11.11.11      Tunnel200002    p1              111     15096
100    33:33:33::33     Tunnel200003    p1               50      7800
```

```
--------------------------------------------------------------------------------
                                                    161     22896
```

How to Configure VxLAN Policing and Accounting

VXLAN Accounting and Policing

The VxLAN policing and accounting can be enabled or disabled according to requirement. If you want to account and police the traffic both through VxLAN static route and VxLAN p2p tunnel enable it using **vxlan static-route accounting-policying bind p2p-tunnel** command.

Before you begin

Prerequisites: Ensure that you have configured VRF and VxLAN static route.

Procedure

	Command or Action	Purpose
Step 1	**vxlan static-route policy output**	Enters VxLAN route policy mode.
Step 2	**vrf vrf1** **Example:** `vxlan static-route`	Enters config-vxlan-route-policy-vrf mode.
Step 3	**police match any vni** *vxlan identifier***rate***traffic bits per second* **Example:** `police match any vni 1 rate 8000`	Specifies the minimum traffic rate for each VNI.

Viewing Accounting and Policing Status

SUMMARY STEPS

1. **show vxlan static-route vni-stats vrf vrf1 vni 1**
2. **show vxlan static-route policy vrf vrf1 vni 1**

DETAILED STEPS

Step 1 **show vxlan static-route vni-stats vrf vrf1 vni 1**

Displays all configurations for a specific VRF.

```
Device# show vxlan static-route vni-stats vrf vrf1 vni 1
VRF: vrf2
Vni Tx-Pkts Tx-Bytes Rx-Pkts Rx-Bytes 1 5000 7140000 50 71400
```

Step 2 **show vxlan static-route policy vrf vrf1 vni 1**

Displays VxLAN static route configurations.

```
Device# show vxlan static-route policy vrf vrf1 vni 1
vrf: vrf1
vni: 1
ref count: 1
obj id: 3
rate: 500000 bps
bc: 15625 bytes
confirmed: 500 pkts,
7140000 bytes; action: transmit exceeded: 0 pkts, 0 bytes; action: drop
```

Information About Ingress and Egress Accounting MIB

From Cisco IOS XE Amsterdam Release 17.2, newly added per VNI/VNET per VRF ingress and engress accounting MIB allows the user to access the counts by SNMP.

Table 99: Ingress and Egress Accounting MIB for per VNI/VNET per VRF

Name	Description
cnvoVNetVrfStatsTable	Table containing all statistics information for the Per VNI/VNET per VRF ingress and egress accounting.
cnvoVNetVrfStatsVrfName	VRF Key to identity count instance. It is not accessible in MIB.
cnvoVNetVrfStatsVni	VNI Key to identity count instance. It is not accessible in MIB.
cnvoVNetVrfIngressPackets	Ingress packets count Per VNI/VNET per VRF. It is not writable.
cnvoVNetVrfIngressBytes	Ingress traffic bytes count Per VNI/VNET per VRF. It is not writable.
cnvoVNetVrfEgressPackets	Engress packets count Per VNI/VNET per VRF. It is not writable.
cnvoVNetVrfEgressBytes	Engress traffic bytes count Per VNI/VNET per VRF. It is not writable.

Configuring the SNMP

The following examples show how to configure SNMP.

Add each VxLAN OID MIB view into the SNMP view:

```
snmp-server view <view-name> cnvoVNetVrfEgressBytes included
snmp-server view <view-name> cnvoVNetVrfEgressPackets included
snmp-server view <view-name> cnvoVNetVrfIngressBytes included
snmp-server view <view-name> cnvoVNetVrfIngressPackets included
```

Or add the table into the SNMP view:

```
snmp-server view <view-name> cnvoVNetVrfStatsTable included
```

Example: SNMP Request for ODI

These examples show the SNMP request for ODI:

Request all ingress packets counters under vrf vrf1:

```
snmpwalk -v 3 -u test -A testpassword -l authNoPriv -a md5 10.75.28.170
1.3.6.1.4.1.9.9.820.1.1.6.1.3.4.118.114.102.49
3:IngressPackets
4: vrf name length
118.114.102.49: vrf name
```

Request ingress packets counters under vrf vrf1 vni 1:

```
snmpget -v 3 -u test -A testpassword -l authNoPriv -a md5 10.75.28.170
1.3.6.1.4.1.9.9.820.1.1.6.1.3.4.118.114.102.49.1
1: vni id
```

Request all counters:

```
snmpwalk -v 3 -u test -A testpassword -l authNoPriv -a md5    10.75.28.170
1.3.6.1.4.1.9.9.820.1.1.6
```

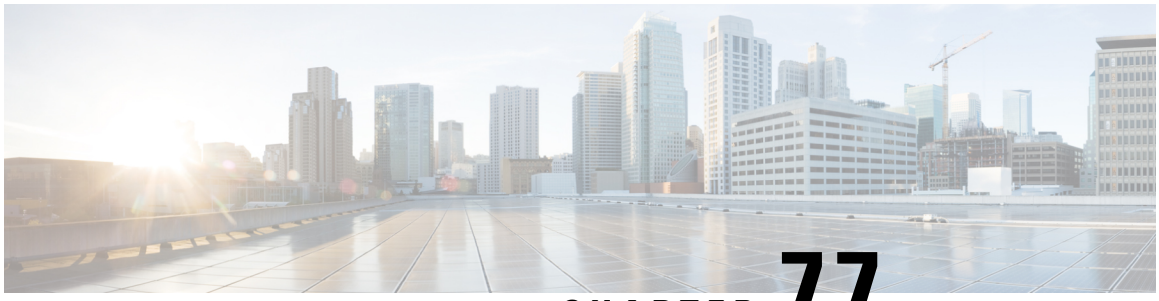
Request all ingress packets counters:

```
snmpwalk -v 3 -u test -A testpassword -l authNoPriv -a md5 10.75.28.170
1.3.6.1.4.1.9.9.820.1.1.6.3
```

For more information on this MIB, see the SNMP Object Navigator.

PART IV

Intelligent Services Gateway



CHAPTER 77

Overview of ISG

Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document provides information about what ISG is, the benefits of ISG, and how to begin implementing it.

Information About ISG

ISG Overview

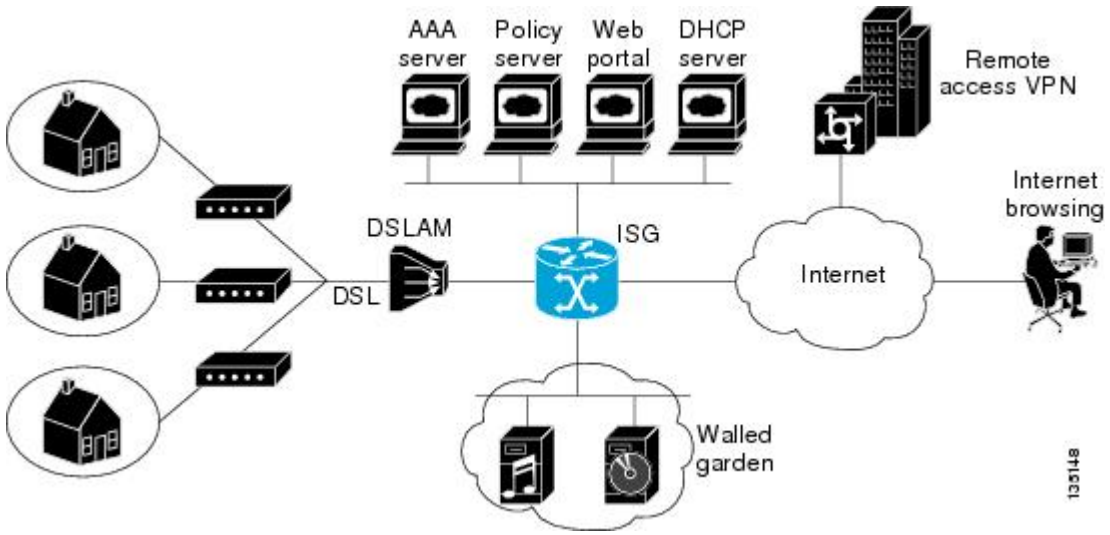
Intelligent Services Gateway (ISG) is a structured framework in which edge access devices deliver flexible and scalable services to subscribers. ISG handles the following key aspects of subscriber management:

- Subscriber identification
- Service and policy determination
- Session policy enforcement
- Session life-cycle management
- Accounting for access and service usage
- Session state monitoring

In addition, ISG introduces a dynamic element to the provisioning and activation of services through control policies and Change of Authorization (CoA) extensions to the RADIUS protocol.

An ISG-enabled device may be deployed at the access edge and service edge of a network and is applicable to a range of subscriber network environments, such as digital subscriber line (DSL), public wireless LAN (PWLAN), and mobile wireless network. Moreover, ISG has been designed to accommodate a flexible distribution of subscriber and service information within a given solution. The figure below illustrates a typical DSL deployment for which service profile data may be stored in an authentication, authorization, and accounting (AAA) database and retrieved and cached on demand.

Figure 55: Sample Topology for a DSL Deployment



It is also possible to define services directly on an ISG. In all cases, service activation may be triggered as a result of a locally defined control policy, user profile associations, or CoA commands from an external policy server or portal application.

Note The IP Base license does not support ISG/PPP/VPDN subscriber features. The minimum feature set for Subscriber support is ADV IP Services or ADV Enterprise Services.

ISG Principles

Fundamental to the ISG architecture is the provisioning of a common session layer at which the management of generic subscriber sessions is decoupled from the technology that is used to provide access to the edge device.

Within this session management layer, common methods are provided for the extraction of subscriber identity information and the determination and activation of services. These methods are described in the following sections:

Subscriber Sessions

An ISG subscriber session is a generic system context that is created for every subscriber who interacts with the edge device. A subscriber session is created on first interaction so that policies may be applied as early as possible. Such policies may facilitate the retrieval of subscriber identity information. All subscriber sessions are assigned a locally unique identifier that may subsequently be used to reference the session.

The session context is the basis for common handling at the session management layer, but the type of traffic that is encompassed in a session context may vary. Broadly, session types may be categorized as Layer 2 or Layer 3, depending on the packet types that are being handled by the session. For instance, a PPP session is a Layer 2 session in that it includes all packets transferred over a link that was established using PPP negotiation. An IP session is Layer 3 because it includes all IP packets exchanged with a subscriber device at a single IP address. Whether a session is Layer 2 or Layer 3 will, to some extent, determine the type of polices that may be activated for the session.

ISG also provides flexibility in terms of how an IP session is defined for an interface. For example, on a particular interface, ISG can be provisioned to classify IP sessions on the basis of a single address (an IP session), a subnet (an IP subnet session), or the interface itself (an IP interface session), wherein all IP packets transferred over the interface are encompassed by the same session.

In a network deployment, ISG session types should be provisioned to represent individual subscriber entities. For example, a particular ISG interface may be directly connected to a subscriber household in which several subscriber devices with individual IP addresses are attached to a household LAN. If the plan is to model each LAN-attached device as a separate subscriber and apply different policies and services to each, the interface should be provisioned to expect IP sessions. However, if the household represents a single subscriber account, and common handling is required for all packets exchanged, the interface should be provisioned as an IP interface or subnet session.

Subscriber Access

Under ISG, the provisioning and handling of specific access media and protocols is decoupled as far as possible from the functionality that is applicable to all session types. This model has the following benefits:

- A common set of subscriber services may be used on an ISG at which heterogeneous subscriber networks are aggregated.
- A common set of subscriber services may be used for multiple ISGs, even when the access technology differs.
- For a given subscriber, the access method may be altered (through provisioning or roaming) without any need to change the service provisioning.
- As new access protocols become available, they can be leveraged by existing edge deployments without requiring changes to the service content; new access protocols plug into the ISG framework.

Subscriber Identification

A subscriber session is created when the first control protocol packet is received from the subscriber device. The control protocol will vary depending on the session type. If there is no control protocol, the session is signaled by the first data packet from the subscriber.

At session start, certain identity information is available, although typically not enough to completely identify the subscriber. Through the use of control policies, the identity information available at session start can be used to drive the extraction of further identity from the subscriber and determine new policy for the session. The following example illustrates how ISG might handle subscriber identity:

- For an IP session, where session start is signaled by a DHCP protocol event, a TCP redirection policy could be activated. This policy would facilitate the collection of a username and credential at an external web portal.

Subscriber Services

An ISG service is a collection of policies applicable to a subscriber session. When a service is activated on a session, all policies contained within that service are activated on the session. Likewise, when a service is deactivated, all policies that are contained within the service are deactivated or removed from the session.

Services are useful for handling fixed policy combinations that are applicable to a number of subscribers. This application reduces duplication of persistent data and allows a group of policies to be activated with a single action and a single reference.

A service may be defined on the edge device directly, through the command-line interface (CLI), or in an external repository and downloaded as required. A downloaded service definition is cached on the device for as long as it is active on one or more sessions.

A service may be activated in one of the following ways:

- As a result of control policy execution
- By receipt of a CoA service-logon command
- By reference in a user profile, where the service is flagged for automatic activation

Services primarily contain traffic policies. There are some restrictions regarding the policies that may be combined in a given service; for example, a service may not contain two traffic policies that specify a different nondefault traffic class unless they apply to different traffic directions (inbound versus outbound).

Where a service contains a network-forwarding policy, it is known as a *primary service* . Only one primary service may be active for a given session at any point in time; that is, primary services are mutually exclusive.

Policies

ISG introduces support for two basic policy types:

- Traffic policies
- Control policies

Traffic policies define the handling of data packets and consist of a traffic class, which defines the packet-based criteria for which the policy is applicable, and one or more traffic actions, which are functional instances that perform specific operations on a data stream and are often referred to as *features* . The traffic actions configured within a traffic policy are invoked for data packets that meet the criteria defined by the traffic class.

Network-forwarding policies are a specific type of traffic policy, for which the action is a network-forwarding action, such as to route packets using a specific virtual routing and forwarding instance (VRF) or to forward packets over a Layer 2 connection. Network-forwarding policies are “classless” in that it is not possible to refine the criteria for which the forwarding action is applicable.

Control policies define the handling of system events and consist of one or more control policy rules and a decision strategy that governs how the constituent policy rules are evaluated. A control policy rule consists of a control class (a flexible condition clause), an event for which the condition is evaluated, and one or more control actions. Control actions are general system functions, such as “authenticate” or “activate a service.”

Control policies may be activated on various targets, such as interfaces or ATM virtual circuits (VCs), and typically control the extraction and authentication of subscriber identity and the activation of services on sessions. Traffic policies may be activated only on sessions and are typically (though not always) applied through service activation.

Control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies represent an intuitive and extensible framework for specifying system behavior. As additional functionality is added to the system, an administrator just has to learn what new events and actions can be included in a control policy, not a completely new set of configuration commands.

Dynamic Policy Updates

Traditionally, subscriber policy has been determined at one point only, at session establishment time, once the principal identity of a subscriber has been authenticated. ISG introduces a dynamic policy model in which session policy may be altered at any time.

Session policy is evaluated at session start and may be reassessed whenever additional identity or service selection information is gleaned from the subscriber via the access protocol. In addition, policy may be updated for a session through the activation of control policies or by means of CoA commands from an external application. In the latter case, the external application may update policy as a result of administrator activity, back-end processing, or subscriber activity (such as service selection at a web portal).

Benefits of ISG

ISG provides the following benefits:

- A common system for session management across Cisco products and access technologies. New access protocols, forwarding protocols, and features may be plugged in with minimal impact and maximum potential for reuse.
- Separation of the concerns of subscriber identification, service application, and subscriber access and session type.
- Flexible session definitions.
- Flexible session detection.
- Flexible, iterative approach to identification, service activation, and policy activation.
- Different trust levels. Session authorization is not contingent on authentication.
- Control policies. Control policies facilitate distributed policy decision-making, reducing round-trip latency between the edge device and policy server, and allow system event handling to be described in a consistent and intuitive manner.
- Common policy model and language for control and traffic policy.
- Provision for dynamic policy updates via CoA (through service activation or “policy push”).
- Use of existing Cisco IOS infrastructure to provide session functionality.
- Use of existing Cisco IOS infrastructure to track session state and life cycle.
- Creation of a session context at first instance of subscriber interaction, thereby facilitating the immediate application of policy to subscriber traffic.
- Flexible distribution of service data.
- Range of accounting options, including prepaid accounting, postpaid accounting, tariff switching for prepaid and postpaid accounting, interim accounting, event-based accounting, and flow-based accounting.
- Single sign-on services to an external application.
- Flexible infrastructure in support of “equal-access” deployments, such as service-based Dynamic Host Configuration Protocol (DHCP) pool and DHCP server determination, dynamic readdressing through DHCP, and VRF transfer.
- Support for standard external interfaces, such as RADIUS and CoA.

Planning for ISG Implementation

ISG is very flexible and supports a wide variety of functionality. Before you begin to configure ISG, you should plan your system carefully. The following sections describe some of the important aspects of your system that you should consider:

Trust Model

Trust levels are determined by the security needs of a particular application domain and the inherent security afforded by the subscriber network. In the following situations, it may not be necessary to authenticate subscriber identity:

- When security is not considered paramount
- When end-to-end security is provided in-band
- When the subscriber network is intrinsically secure

Whether or not subscribers must be authenticated will influence the choice of access protocol. When authentication is not required, control policies may be used to determine authorization and other session policy on the basis of subscriber identity.

Where authentication is considered necessary, the authenticated identity may be trusted:

- For the duration of the session
- Until a periodic reauthentication is instigated
- Beyond the duration of a session; for example, for the lifetime of a subscription

For complete security, cryptographic methods may be used to secure the session (to the edge) following authentication, obviating the need for reauthentication. However, there are administrative and performance overheads associated with this practice.

Subscriber Access Model

The trust model will, to a large extent, determine the choice of access protocol. However, the access model will also depend on other factors such as the underlying media (for example, ATM versus Ethernet), type of endpoint (for example, PC, cell phone, PDA), mobility requirements, the system's ability to influence the software installed on a subscriber device, and scalability requirements.

Single Sign-On Requirements

Where a subscriber will have access to services provided by other devices in the administrative domain of the access or service provider, is an additional authentication required, or should the identity of the subscriber be trusted? It may be necessary for the latter device to query the access device to collect additional subscriber identity information and ascertain whether the subscriber has already been authenticated by the access device. The single sign-on facility is provided through the "session query" capability of CoA.

Network Forwarding

How should subscribers be given access to network services? Network forwarding options include the following:

- Layer 2 connections; for example, a Layer 2 Tunneling Protocol (L2TP) tunnel to an L2TP network server (LNS)

- Layer 3 connections, by associating all session packets with a particular VRF or routing domain

Service Packaging

How should subscriber policies be organized into services, if at all? Some considerations for service packaging include the following:

- Are certain policy combinations common to multiple subscribers?
- Are shared policy combinations dependent on a particular forwarding domain?
- Is it necessary for a subscriber to move between service domains?
- Should services be defined on the device or in a remote repository? Externally defined services will be cached locally for as long as they are activated for one or more sessions.

Billing Model

How should subscribers be billed for service usage? Billing options include the following:

- Billing by usage of time or volume
- Billing in advance (prepaid) or at regular intervals (traditional postpaid)
- Billing according to policies provisioned for the session
- Billing according to the time of day (tariff switching)

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

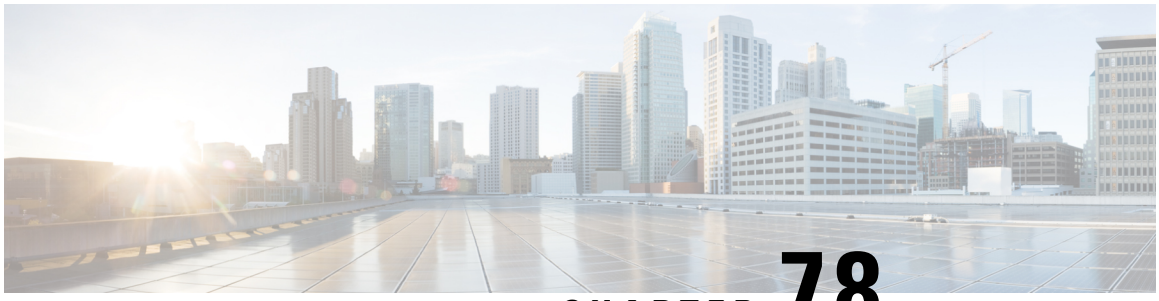
Feature Information for the Overview of ISG

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 100: Feature Information for the Overview of ISG

Feature Name	Releases	Feature Configuration Information
ISG:Session: Auth: Single Sign-on	Cisco IOS XE Release 2.2.	Single sign-on eliminates the need to authenticate a session more than once when a subscriber has access to services provided by other devices in the administrative domain of the access or service provider.



CHAPTER 78

Configuring ISG Control Policies

Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG control policies are a means of defining the actions the system will take in response to specified conditions and events. A wide variety of system actions, conditions, and events can be combined using a consistent policy language, providing a flexible and precise way of configuring ISG. This module provides information about how to configure ISG control policies.

Prerequisites for ISG Control Policies

Authentication, authorization, and accounting (AAA) method lists must be configured prior to defining authentication and authorization actions.

Restrictions for ISG Control Policies

Control policies are activated for specific contexts, not directly on sessions. Control policies apply to all sessions hosted on the context.

Only one control policy map may be applied to a given context.

Control policies can be defined only through the router's command-line interface (CLI).

Not all actions may be associated with all events.

A new control class may not be inserted between existing control classes once a control policy map has been defined.

Changing the ISG configuration service-policy on interfaces having active sessions is not supported and may result in session state inconsistency or device reload. We recommend to shut down all ISG interfaces with active sessions before performing any configuration changes on the ISG service-policy.

Information About ISG Control Policies

Control Policies

Control policies define the actions that the system will take in response to specified events and conditions. For example, a control policy can be configured to authenticate specific subscribers and then provide them with access to specific services.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions will be executed.

Three steps are involved in defining a control policy:

1. Create one or more control class maps—A control class map specifies the conditions that must be met for a policy to be activated, and, optionally, the event that causes the class to be evaluated. A control class map may contain multiple conditions, each of which will evaluate to either true or false. Match directives can be used to specify whether all, any, or none of the individual conditions must evaluate true in order for the class to evaluate true.
2. Create a control policy map—A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.
3. Apply the control policy map—A control policy map is activated by applying it to a context. A control policy map can be applied to one or more of the following types of contexts. In the following list, the context types are listed in order of precedence. For example, a control policy map that is applied to a PVC takes precedence over a control policy map that is applied to an interface.
    - Permanent virtual circuit (PVC)
    - Virtual circuit (VC) class
    - Virtual template
    - Subinterface
    - Interface
    - Global

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts.

Note Traffic policies are another type of policy used by ISG. Traffic policies define the handling of data packets and are configured in service policy maps or service profiles. For more information about traffic policies, see the "Configuring ISG Subscriber Services" module.

Differentiated Initial Policy Control

Authentication failure for a subscriber may happen for an access-reject (which means a RADIUS server responded with a Reject) or due to an access request timeout (RADIUS server is unreachable).

Using ISG control policies, and actions configured for the 'radius-timeout' and 'access-reject' events, the system can distinguish between the different reasons for an authentication failure. Different events are thrown by the system (for example, a received authentication reject or an unavailable RADIUS server event). This allows the control policy to specify different actions for each type of authentication failure. For example, if the RADIUS server is down or unreachable, temporary access can be given to subscribers.

This feature is available only for IP-based sessions for subscriber authentication. This feature does not support the Point-to-Point Protocol over Ethernet (PPPoE) sessions.

Uses of Control Policies

Use control policies to configure an ISG to perform specific actions in response to specific events and conditions. For example, control policies could be used for the following purposes:

- To activate a default service when a subscriber session is first detected
- To sequence the gathering of subscriber identity, where a control protocol exists on the access side
- To determine how the system responds to an idle timeout or to a subscriber who has run out of credit
- To enable transparent automatic login, which enables authorization on the basis of an IP address or MAC address
- To configure the maximum amount of time a session can remain unauthenticated
- To send periodic session state information to other devices

HA Support for ISG Control Policies

The ISG Policy HA and RADIUS-Based Policing HA feature adds stateful switchover (SSO) and In Service Software Upgrade (ISSU) support to ISG control policies.

For information about configuring high availability (HA) on the ISG router, see the High Availability Configuration Guide, Cisco IOS XE Release 3S.

How to Configure an ISG Control Policy

Configuring a Control Class Map

A control class map contains conditions that must be met for a control policy to be executed. A control class map can contain one or more conditions. Perform this task to configure a control class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name*
4. **available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}

5. **greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
6. **greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
7. **less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
8. **less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
9. **match authen-status** {**authenticated** | **unauthenticated**}
10. **match authenticated-domain** {*domain-name* | **regexp** *regular-expression*}
11. **match authenticated-username** {*username* | **regexp** *regular-expression*}
12. **match dnis** {*dnis* | **regexp** *regular-expression*}
13. **match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**}
14. **match mlp-negotiated** {**no** | **yes**}
15. **match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*}
16. **match no-username** {**no** | **yes**}
17. **match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**}
18. **match service-name** {*service-name* | **regexp** *regular-expression*}
19. **match source-ip-address** *ip-address subnet-mask*
20. **match timer** {*timer-name* | **regexp** *regular-expression*}
21. **match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*}
22. **match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*}
23. **match unauthenticated-username** {*username* | **regexp** *regular-expression*}
24. **match vrf** {*vrf-name* | **regexp** *regular-expression}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**class-map type control** [**match-all**|**match-any**|**match-none**] *class-map-name* **Example:** `Router(config)# class-map type control match-all class1`	Creates or modifies a control class map, which defines the conditions under which the actions of a control policy map will be executed, and enters control class map mode.
Step 4	**available** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **Example:** `Router(config-control-classmap)# available nas-port`	(Optional) Creates a condition that evaluates true if the specified subscriber identifier is locally available.
Step 5	**greater-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **Example:** `Router(config-control-classmap)# greater-than nas-port type atm vpi 200 vci 100`	(Optional) Creates a condition that evaluates true if the subscriber network access server (NAS) port identifier is greater than the specified value.
Step 6	**greater-than-or-equal** [**not**]**nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **Example:** `Router(config-control-classmap)# greater-than-or-equal nas-port vlan 10`	(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is greater than or equal to the specified value.
Step 7	**less-than** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **Example:** `Router(config-control-classmap)# less-than nas-port type atm vpi 200 vci 105`	(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than the specified value.

	Command or Action	Purpose
Step 8	**less-than-or-equal** [**not**] **nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **ipaddr** *ip-address* | **port** *port-number* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** *interface-type* | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **Example:** `Router(config-control-classmap)# less-than-or-equal nas-port ipaddr 10.10.10.10`	(Optional) Creates a condition that evaluates true if the specified subscriber NAS port identifier is less than or equal to the specified value.
Step 9	**match authen-status** {**authenticated** | **unauthenticated**} **Example:** `Router(config-control-classmap)# match authen-status authenticated`	(Optional) Creates a condition that evaluates true if a subscriber's authentication status matches the specified authentication status.
Step 10	**match authenticated-domain** {*domain-name* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match authenticated-domain cisco.com`	(Optional) Creates a condition that evaluates true if a subscriber's authenticated domain matches the specified domain.
Step 11	**match authenticated-username** {*username* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match authenticated-username regexp "admin@.*com"`	(Optional) Creates a condition that evaluates true if a subscriber's authenticated username matches the specified username.
Step 12	**match dnis** {*dnis* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match dnis reg-exp 5551212`	(Optional) Creates a condition that evaluates true if a subscriber's Dialed Number Identification Service number (DNIS number, also referred to as *called-party number*) matches the specified DNIS number.
Step 13	**match media** {**async** | **atm** | **ether** | **ip** | **isdn** | **mpls** | **serial**} **Example:** `Router(config-control-classmap)# match media atm`	(Optional) Creates a condition that evaluates true if a subscriber's access media type matches the specified media type.
Step 14	**match mlp-negotiated** {**no** | **yes**} **Example:** `Router(config-control-classmap)# match mlp-negotiated yes`	(Optional) Creates a condition that evaluates true or false depending on whether the subscriber's session was established using multilink PPP negotiation. • If the **yes** keyword is used, the condition evaluates true if the subscriber's session was established using multilink PPP negotiation.

	Command or Action	Purpose
Step 15	**match nas-port** {**adapter** *adapter-number* | **channel** *channel-number* | **circuit-id** *name* | **ipaddr** *ip-address* | **port** *port-number* | **remote-id** *name* | **shelf** *shelf-number* | **slot** *slot-number* | **sub-interface** *sub-interface-number* | **type** {**async** | **atm** | **basic-rate**| **enm** | **ether** | **fxo** | **fxs** | **none** | **primary-rate** | **synch** | **vlan** | **vty**} | **vci** *vci-number* | **vlan** *vlan-id* | **vpi** *vpi-number*} **Example:** `Router(config-control-classmap)# match nas-port type ether slot 3`	(Optional) Creates a condition that evaluates true if a subscriber's NAS port identifier matches the specified value.
Step 16	**match no-username** {**no** | **yes**} **Example:** `Router(config-control-classmap)# match no-username yes`	(Optional) Creates a condition that evaluates true or false depending on whether or not a subscriber's username is available. • If the **yes** keyword is used, the condition evaluates true if the subscriber's username is not available.
Step 17	**match protocol** {**atom** | **ip** | **pdsn** | **ppp** | **vpdn**} **Example:** `Router(config-control-classmap)# match protocol ip`	(Optional) Creates a condition that evaluates true if a subscriber's access protocol type matches the specified protocol type.
Step 18	**match service-name** {*service-name* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match service-name service1`	(Optional) Creates a condition that evaluates true if the service name associated with a subscriber matches the specified service name.
Step 19	**match source-ip-address** *ip-address subnet-mask* **Example:** `Router(config-control-classmap)# match source-ip-address 10.10.10.10 255.255.255.255`	(Optional) Creates a condition that evaluates true if a subscriber's source IP address matches the specified IP address.
Step 20	**match timer** {*timer-name* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match timer TIMERA`	(Optional) Creates a condition that evaluates true upon expiry of a specified policy timer.
Step 21	**match tunnel-name** {*tunnel-name* | **regexp** *regular-expression*} **Example:**	(Optional) Creates a condition that evaluates true if a subscriber's virtual private dialup network (VPDN) tunnel name matches the specified tunnel name.

	Command or Action	Purpose
	`Router(config-control-classmap)# match tunnel-name regexp L.*`	
Step 22	**match unauthenticated-domain** {*domain-name* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match unauthenticated-domain example.com`	(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated domain name matches the specified domain name.
Step 23	**match unauthenticated-username** {*username* | **regexp** *regular-expression*} **Example:** `Router(config-control-classmap)# match unauthenticated-username regexp examplename1`	(Optional) Creates a condition that evaluates true if a subscriber's unauthenticated username matches the specified username.
Step 24	**match vrf** {*vrf-name* | **regexp** *regular-expression}* **Example:** `Router(config-control-classmap)# match vrf regexp examplename2`	(Optional) Creates a condition that evaluates true if a subscriber's VPN routing and forwarding (VRF) matches the specified VRF.

Configuring a Control Policy Map

A control policy map contains one or more control policy rules that associate a control class with one or more actions. Perform this task to configure a control policy map.

Note The actions that can be configured in a policy rule depend on the type of event that is specified by the **class type control** command. For example, if the **account-logoff** event is specified, the only action that can be configured in that policy rule is **service**. The procedure in this section shows all actions that can be configured in a policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff** | **account-logon** | **acct-notification** | **credit-exhausted** | **dummy-event** | **flow-timeout** | **quota-depleted** | **radius-timeout** | **service-failed**| **service-start** | **service-stop** | **session-default-service** | **session-restart** | **session-service-found** | **session-start** | **timed-policy-expiry**}]
5. *action-number* **authenticate aaa list** *list-name*
6. *action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**}[**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier**

{**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**}

7. *action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username | vrf**}
8. *action-number* **if upon network-service-found** {**continue** | **stop**}
9. *action-number* **proxy accounting aaa list** {*list-name*| **default**}
10. *action-number* **service** [**disconnect** | **local** | **vpdn**]
11. *action-number* **service-policy type control** *policy-map-name*
12. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** |**unauthenticated-domain** | **unauthenticated-username**}}
13. *action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**|**vrf**}
14. *action-number* **set-timer** *name-of-timer minutes*
15. *action-number* **substitute** *name matching-pattern pattern-string*
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	**class type control** {*control-class-name* | **always**} [**event** {**access-reject**| **account-logoff**	**account-logon**	**acct-notification**	**credit-exhausted**	**dummy-event**	**flow-timeout**	**quota-depleted**	**radius-timeout**	**service-failed**| **service-start**	**service-stop**	**session-default-service**	**session-restart**	**session-service-found**	**session-start**	**timed-policy-expiry**}]	Specifies a control class for which actions may be configured. • A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.

	Command or Action	Purpose
	Example: `Router(config-control-policymap)# class type control always event session-start`	
Step 5	*action-number* **authenticate aaa list** *list-name* **Example:** `Router(config-control-policymap-class-control)# 1 authenticate aaa list LIST1`	(Optional) Initiates an authentication request.
Step 6	*action-number* **authorize use method** {**aaa**|**legacy**|**rm**|**sgf**|**ssg**|**xconnect**} [**aaa** *parameter-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect**| **circuit-id**| **dnis** | **mac-address** | **nas-port** | **remote-id**| **source-ip-address** | **tunnel-name**| **unauthenticated-domain** | **unauthenticated-username**|**vendor-class-id**} **Example:** `Router(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`	(Optional) Initiates a request for authorization on the basis of the specified identifier.
Step 7	*action-number* **collect** [**aaa list** *list-name*] **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address** | **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username** | **vrf**} **Example:** `Router(config-control-policymap-class-control)# 1 collect identifier authen-status`	(Optional) Collects the specified subscriber identifier from the access protocol.
Step 8	*action-number* **if upon network-service-found** {**continue** | **stop**} **Example:** `Router(config-control-policymap-class-control)# 2 if upon network-service-found stop`	(Optional) Specifies whether the system should continue processing policy rules once the subscriber's network service has been identified.
Step 9	*action-number* **proxy accounting aaa list** {*list-name*| **default**} **Example:** `Router(config-control-policymap-class-control)# 1 proxy accounting aaa list default`	(Optional) Specifies the list that the request should be proxied to.

	Command or Action	Purpose
Step 10	*action-number* **service** [**disconnect** | **local** | **vpdn**] **Example:** `Router(config-control-policymap-class-control)# 3 service disconnect`	(Optional) Specifies a network service type for PPP sessions.
Step 11	*action-number* **service-policy type control** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# service-policy type control domain based access`	(Optional) Nests the specified control policy map within a parent control policy map.
Step 12	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** |**unauthenticated-domain** | **unauthenticated-username**}} **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`	(Optional) Activates an ISG service. • Specifying an identifier instead of a service name will activate a service that has the same name as the specified identifier.
Step 13	*action-number* **set** *name* **identifier** {**authen-status** | **authenticated-domain** | **authenticated-username** | **dnis** | **mac-address**| **media** | **mlp-negotiated** | **nas-port** | **no-username** | **protocol** | **service-name** | **source-ip-address** | **timer** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**|**vrf**} **Example:** `Router(config-control-policymap-class-control)# 1 set APJ identifier authen-status`	(Optional) Sets a variable name.
Step 14	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Router(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy-expiry.
Step 15	*action-number* **substitute** *name matching-pattern pattern-string* **Example:** `Router(config-control-policymap-class-control)# 1 substitute TPK SUBA SUBB`	(Optional) Substitutes a matching pattern in variable content by a rewrite pattern.

	Command or Action	Purpose
Step 16	**end** **Example:** `Router(config-control-policymap-class-control)# end`	(Optional) Ends the current configuration session and returns to privileged EXEC mode.

Applying the Control Policy Map

A control policy map must be activated by applying it to a context. Perform one or more of the following tasks to apply a control policy to a context:

Applying a Control Policy Map Globally on the Router

Perform this task to apply a control policy globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-policy type control** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service-policy type control** *policy-map-name* **Example:** `Router(config)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to an Interface or Subinterface

Perform this task to apply an ISG control policy to an interface or subinterface.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface** *type number* [**.** *subinterface-number*]
4. **service-policy type control** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [**.** *subinterface-number*] **Example:** `Router(config)# interface gigabitethernet 0/0/1.1`	Specifies an interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Applying an ISG Control Policy Map to a Virtual Template

Perform this task to apply an ISG control policy map to a virtual template.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **service-policy type control** *policy-map-name*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template0`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control policy1`	Applies a control policy.

Monitoring and Maintaining ISG Control Policies

Optionally, you can perform this task to monitor and maintain ISG control policy operation. Steps can be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show class-map type control**
3. **show policy-map type control**
4. **clear class-map control**
5. **clear policy-map control**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map type control** **Example:** `Router# show class-map type control`	Displays information about ISG control class maps. • The display includes statistics on the number of times a particular class has been evaluated and what the results were.
Step 3	**show policy-map type control** **Example:**	Displays information about ISG control policy maps.

	Command or Action	Purpose
	`Router# show policy-map type control`	• The display includes statistics on the number of times each policy rule within the policy map has been executed.
Step 4	**clear class-map control** **Example:** `Router# clear class-map control`	Clears the control class map counters.
Step 5	**clear policy-map control** **Example:** `Router# clear policy-map control`	Clears the control policy map counters.

Configuration Examples for ISG Control Policies

Control Policy for Layer 2 Access and Service Provisioning Example

The following example shows how to configure a control policy that produces the following results:

- VPDN forwarding is applied to anyone dialing in from “example1.com”.
- Access to locally terminated Layer 3 network resources is provided to anyone dialing in from “example2.com”.
- Anyone else is barred.

```
! Configure the control class maps.
class-map type control match-all MY-FORWARDED-USERS
 match unauthenticated-domain "example1.com"
!


class-map type control match-all MY-LOCAL-USERS
 match unauthenticated-domain "example2.com"
!
! Configure the control policy map.
policy-map type control MY-POLICY
 class type control MY-FORWARDED-USERS event session-start
  1 service-policy type service identifier nas-port
  2 service local
!
 class type control MY-LOCAL-USERS event session-start
  1 service local
!
 class type control always event session-start
  2 service disconnect
!
! Apply the control policy to dialer interface 1.
interface Dialer1
 service-policy type control MY-POLICY
```

Verifying a Control Policy Examples

The following examples show sample output generated from the configuration in the Control Policy for Layer 2 Access and Service Provisioning Example:

```
Router# show users

Line User Host(s) Idle Location
* 0 con 0 idle 00:00:00
Interface User Mode Idle Peer Address
Vi1.1 user1@xyz.com PPPoE - 10.1.126.14
Vi1.2 user2@abc.com PPPoE - 10.1.126.15

Router# show subscriber session

Current Subscriber Information: Total sessions 2
Uniq ID Interface State Service Identifier Up-time
2022 Vi1.1 authen Local Term user1@xyz.com 00:08:41
2023 Vi1.2 authen Local Term user2@abc.com 00:08:40
MCP_BBA_8#show subscriber session
MCP_BBA_8#show subscriber session uid 2022 detailed
Unique Session ID: 2022
Identifier: user1@xyz.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:08:57, Last Changed: 00:08:57
Interface: Virtual-Access1.1
Policy information:
Context 2C655DF0: Handle A2070D8D
AAA_id 00007DE8: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
1 service local
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
```

```
Session inbound features:
Feature: Policing
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:56
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:03
Router# show subscriber session uid 2023 detailed
Unique Session ID: 2023
Identifier: user2@abc.com
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:09:17, Last Changed: 00:09:17
Interface: Virtual-Access1.2
Policy information:
Context 2C656120: Handle F4070D8E
AAA_id 00007DE9: Flow_handle 0
Authentication status: authen
Downloaded User profile, excluding services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Downloaded User profile, including services:
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Config history for session (recent to oldest):
Access-type: PPP Client: SM
Policy event: Process Config Connecting
Profile name: apply-config-only, 3 references
service-type 2 [Framed]
Framed-Protocol 1 [PPP]
timeout 720 (0x2D0)
ssg-account-info ''QU;10000;D;20000''
Rules, actions and conditions executed:
subscriber rule-map ppp-users
condition always event session-start
1 collect identifier unauthenticated-domain
2 service-policy type control MY-POLICY
subscriber condition-map match-all MY-FORWARDING-USERS
match identifier unauthenticated-domain xyz.com [FALSE]
subscriber rule-map MY-POLICY
condition MY-FORWARDING-USERS event session-start
subscriber condition-map match-all MY-LOCAL-USERS
match identifier unauthenticated-domain abc.com [TRUE]
subscriber rule-map MY-POLICY
condition MY-LOCAL-USERS event session-start
1 service local
subscriber rule-map ppp-users
condition always event session-start
2 service-policy type control MY-POLICY
Session inbound features:
Feature: Policing
```

```
Upstream Params:
Average rate = 10000, Normal burst = 1875, Excess burst = 3750
Config level = Per-user
Session outbound features:
Feature: Policing
Dnstream Params:
Average rate = 20000, Normal burst = 3750, Excess burst = 7500
Config level = Per-user
Non-datapath features:
Feature: Session Timeout
Timeout value is 720 seconds
Time remaining is 00:02:40
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:09:19
```

Control Policy for Restricting Access on the Basis of Interface and Access Media Example

This example shows how to configure a control policy to allow access only to users who enter the router from a particular interface and access type. In this case, only PPPoE users will be allowed; everyone else is barred.

The first condition class map “MATCHING-USERS” evaluates true only if all of the lines within it also evaluate true; however, within “MATCHING-USERS” is a nested class map (second condition), “NOT-ATM”. This nested class map represents a subcondition that must also evaluate to true. Note that the class map “NOT-ATM” specifies “match-none”. This means that “NOT-ATM” evaluates to true only if every condition line within it evaluates to false.

The third condition specifies matching on the NAS port associated with this subscriber. Specifically, only subscribers that arrive on a Gigabit Ethernet interface and on slot 3 will evaluate to true.

```
! Configure the control class maps.
class-map type control match-all MATCHING-USERS
 class type control NOT-ATM
 match media ether
 match nas-port type ether slot 3
!
class-map type control match-none NOT-ATM
 match media atm
!
```

If the conditions in the class map “MATCHING-USERS” evaluate to true, the first action to be executed is to authenticate the user. If authentication is successful, the service named “service1” will be downloaded and applied. Finally, a Layer 3 service is provided.

If “MATCHING-USERS” is not evaluated as true, the “always” class will apply, which results in barring anyone who does not match “MATCHING-USERS”.

```
! Configure the control policy map.
policy-map type control my-pppoe-rule
 class type control MATCHING-USERS event session-start
  1 authenticate aaa list XYZ
  2 service-policy type service service1
  3 service local
!
```

class type control always

```
  1 service disconnect
```

```
!
! Apply the control policy to an interface.
interface gigabitethernet3/0/0
 service-policy type control my-pppoe-rule
```

Finally, the policy is associated with an interface.

Default Method Lists

If you specify the default method list for any of the control policy actions, the default list will not display in the output from the **show running-config** command. For example, if you configure the following command:

```
Router(config-control-policymap-class-control)# 1 authenticate aaa list default
```

The following will display in the output from the **show running-config** command:

```
1 authenticate
```

Control Policies for Automatic Subscriber Login Example

In the following example, if the client is from the a subnet, automatic subscriber login is applied and an authorization request is sent to the list TALLIST with the subscriber's source IP address as the username. If the authorization request is successful, any automatic activation services specified in the returned user profile are activated for the session and the execution of rules within the control policy stops. If the authorization is not successful, the rule execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

```
interface GigabitEthernet0/0/0
 service-policy type control RULEA
aaa authentication login TALLIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
```

policy-map type service redirectprofile

```
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 209.165.201.1 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 apply aaa list LOCAL service redirectprofile
  3 set-timer TIMERB 5 minutes
 class type control CONDF event timed-policy-expiry
```

1 service disconnect

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS High Availability Configuration Guide*
Traffic Policies	"Configuring ISG Subscriber Services" module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

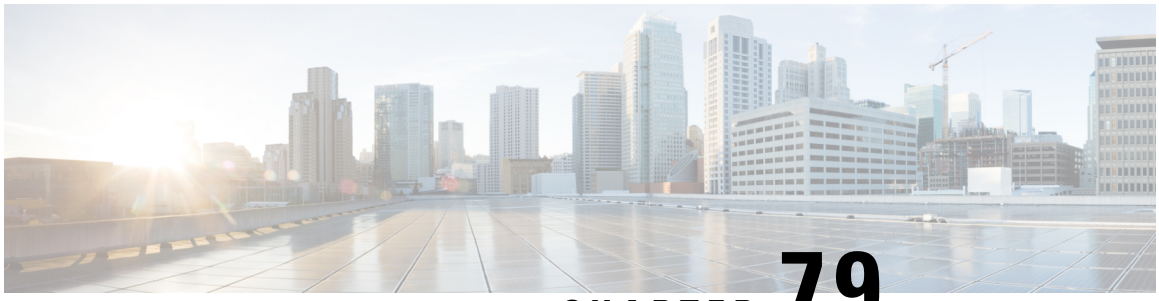
Feature Information for ISG Control Policies

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 101: Feature Information for ISG Control Policies

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Policy: Domain Based (Autodomain, Proxy)	Cisco IOS XE Release 2.2	ISG control policies manage the primary services and rules used to enforce particular contracts. These policies include programmable interfaces to dynamic triggers and conditional logic to be applied to flows within a session, or other characteristics of a session, upon meeting the policy criteria. Policies can be configured to interpret the domain as a request to activate the service associated with that domain name, allowing users to automatically receive services in accordance with the domain to which they are attempting to connect.
ISG: Policy Control: Policy: Triggers	Cisco IOS XE Release 2.2	ISG control policies can be configured with time-based, volume-based, and duration-based policy triggers. Time-based triggers use an internal clock, allowing policies to be applied at specific times. Volume-based triggers are based on packet count; when the packet count reaches a specified value, the specified policy is applied. Duration-based triggers are based on an internal timer. Upon expiration of the timer, the specified policy is applied.
ISG: Policy Control: Multidimensional Identity per Session	Cisco IOS XE Release 2.2	ISG control policies provide a flexible way to collect pieces of subscriber identity information during session establishment. Control policies also allow session policy to be applied iteratively as more elements of identity information become available to the system.
ISG: Policy Control: Cisco Policy Language	Cisco IOS XE Release 2.2	ISG control policies are a structured replacement for feature-specific configuration commands and allow configurable functionality to be expressed in terms of an event, a condition, and an action. Control policies provide an intuitive and extensible framework, with a consistent set of CLI commands, for specifying system behavior.
ISG: Policy Control: Differentiated Initial Policy Control	Cisco IOS XE Release 2.5.0	This features provides the ability to distinguish RADIUS authentication rejects from RADIUS server unavailability. It allows minimal or temporary network access to the subscribers when the RADIUS servers are down or cannot be accessed because of network problems or when an authentication reject is received for a subscriber. In Cisco IOS Release 12.2(33)XNE, support was added for the Cisco 10000 Series Routers. The following command was introduced or modified:**class type control**.
ISG Policy HA and RADIUS-Based Policing HA	Cisco IOS XE Release 3.5S	Adds SSO and ISSU support to the ISG policy manager.



CHAPTER 79

Configuring ISG Access for PPP Sessions

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document provides information about how to configure ISG access for Point-to-Point Protocol (PPP) subscribers.

Prerequisites for ISG Access for PPP Sessions

The specific access protocol that is being used must be provisioned on the interface.

If local PPP authentication is required, the **ppp authentication** command must be configured on the interface or virtual template.

The tasks and examples in this document assume that you know how to configure and use ISG control policies. See the module “Configuring ISG Control Policies” for information about how to configure control policies.

Restrictions for ISG Access for PPP Sessions

The idle timeout value configured with the **ppp timeout idle** command in a virtual template applies to a PPP session even when the session is forwarded.

Information About ISG Access for PPP Sessions

Overview of ISG Access for PPP Sessions

Layer 2 sessions are established by means of control protocols that operate between the peer entities and the ISG device. Typically, Layer 2 sessions are encapsulated to isolate them from other sessions on the same physical media.

Although the system provides default handling for Layer 2 sessions, you may want to configure policies to forward or locally terminate the protocol or to locally authenticate subscribers on the basis of identity data that is collected from the access protocol. ISG control policies can be configured to extract identity and credentials of peer entities from access protocols. This mechanism allows services to be provisioned for Layer 2 sessions on the basis of any identity pertaining to the session, whether explicitly provided via the protocol or native to the underlying media or access port.

ISG supports the following Layer 2 access protocols:

- PPP
- PPP over Ethernet (PPPoE)
- Layer 2 Tunnel Protocol (L2TP)

ISG Subscriber IP Address Management for PPP Sessions

ISG subscriber IP address management applies to IP sessions or Layer 2 (PPP) sessions that are terminated locally.

For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (which includes any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain. For locally terminated PPP sessions, ISG supports the following methods of IP address assignment:

- IP address in a user profile
- IP subnet in a user profile
- Named address pool in a user profile
- Local address pools
- Standard methods of IP address management for PPP

When a locally terminated PPP session is transferred from one virtual routing and forwarding (VRF) instance to another VRF, the peer IP address is renegotiated using IPCP.

VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another following selection of a new primary service. Once a PPP session comes up with the IP address from the network access point (NAP), the subscriber can access a web portal and choose a service provider. On VRF transfers in PPP sessions, ISG

must reassign the IP address from the new domain to the PPP session. In PPP sessions, the IP address is reassigned by IP Control Protocol (IPCP) renegotiation.

Without PPP renegotiation, VRF transfer is not supported for PPP sessions.

Default Policy for ISG Access for PPP Sessions

ISG provides default handling of Layer 2 sessions in the absence of a configured control policy. If the **vpdn enable** command is configured and a domain name is specified in the username (for example, user@domain) or a Dialed Number Identification Service (DNIS) number has been provided, the system will perform authorization on the basis of this information. If virtual private dialup network (VPDN) tunnel information is found, the session will be forwarded for handling at an L2TP network server (LNS). If authentication is required by the remote LNS, the **ppp authentication** command must be configured at the PPP interface or virtual template. If the **vpdn authen-before-forward** command is configured, the system will attempt to authenticate the PPP session locally before forwarding it on to the LNS.

If tunnel information is not found for the domain name or DNIS or the **vpdn enable** command is not configured, Stack Group Bidding Protocol (SGBP) authorization will be attempted (if SGBP is configured). If no authorization information is located using SGBP, the PPP session will be terminated locally. Local termination means that the PPP session will be established between the peer and the ISG device, and the IP payload will be routed. In the latter case, authentication will occur only if the **ppp authentication** command is configured on the PPP interface or virtual template.

If an ISG control policy is defined for the session-start event, that policy will override the default handling.

How to Configure ISG Access for PPP Sessions Using Control Policies

To configure ISG Layer 2 access, perform the following steps:

1. Decide how you want Layer 2 session handling to be influenced by subscriber identity. Do you want to forward the protocol or terminate it locally? Do you want to authenticate subscribers locally?
2. Configure control policies to provide Layer 2 session handling. See the module "Configuring ISG Control Policies" for information about how to configure control policies. See the "Configuration Examples for ISG Access for PPP Sessions" section for an example of a control policy for Layer 2 access.
3. Enable ISG VRF transfer for PPP sessions.
4. Verify and troubleshoot the configuration as needed.

This section contains the following tasks:

Enabling ISG VRF Transfer for PPP Sessions

VRF transfer enables an ISG subscriber session to move from one VRF to another when a new primary service is activated for a session. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

Before you begin

This procedure assumes that you have configured support for PPP sessions by configuring a virtual template and method of IP address allocation. Note that the original VRF, loopback interface, and IP address pool must be specified in a virtual template rather than in a user profile in order for VRF transfer to work. For information about how to configure virtual templates and support for PPP sessions, see the *Cisco IOS XE Dial Technologies Configuration Guide.*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service is a service that contains a network-forwarding policy. A primary service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

	Command or Action	Purpose
Step 6	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a grouping of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.

Verifying VRF Transfer for PPP Sessions

Perform this task to verify VRF transfer for PPP sessions. All of the **show** steps are optional and may be performed in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
4. **show ip route** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays information pertaining to the service chosen by the subscriber.
Step 3	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]]	**service key session-handle** *session-handle-string* **service-key** *key-value*	**session key** {**aaa-unique-id** *aaa-unique-id-string*	**domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*| **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id*	**portbundle ip** *ip-address* **bundle** *bundle-number*	**session-guid** *session-guid*	**session-handle** *session-handle-string*	**session-id** *session-id-string*}	**statistics**} **Example:**	Displays information related to ISG session and service identity.

	Command or Action	Purpose
	`Router# show idmgr session key session-handle 48000002`	
Step 4	**show ip route** [**vrf** *vrf-name*] **Example:** `Router# show ip route`	Displays the current state of the routing table.

Troubleshooting ISG Access for PPP Sessions

The commands in this task can be used to monitor and troubleshoot Layer 2 sessions. All of these commands are optional and do not need to be entered in a particular order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session detailed**
3. **debug condition** *condition*
4. **debug subscriber packet** [**event**| **full**| **detail**]
5. **debug subscriber error**
6. **debug subscriber event**
7. **debug subscriber fsm**
8. **debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session detailed** **Example:** `Router# show subscriber session detailed`	Displays information about ISG subscriber sessions.
Step 3	**debug condition** *condition* **Example:** `Router# debug condition username user5@isp.com`	Filters debug output on the basis of the specified condition. **Note** See the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging" for information about conditional debugging.
Step 4	**debug subscriber packet** [**event**| **full**| **detail**] **Example:**	Displays diagnostic information about packets during Subscriber Service Switch (SSS) call setup.

	Command or Action	Purpose
	`Router# debug subscriber packet event`	
Step 5	**debug subscriber error** **Example:** `Router# debug subscriber error`	Displays diagnostic information about errors that can occur during SSS call setup.
Step 6	**debug subscriber event** **Example:** `Router# debug subscriber event`	Displays diagnostic information about SSS call setup events.
Step 7	**debug subscriber fsm** **Example:** `Router# debug subscriber fsm`	Displays diagnostic information about the SSS call setup state.
Step 8	**debug ppp** {**packet** | **negotiation** | **error** | **authentication** | **subscriber switch**} **Example:** `Router# debug ppp packet`	Displays information on traffic and exchanges in an internetwork that is implementing the PPP.

Example

In the following example, the output of the **debug subscriber packet detail** command is filtered on the basis of the username “cpe6_1@isp.com”:

```
Router# debug condition username cpe6_1@isp.com
Condition 1 set
Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on
Router# show debug
SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)
```

Configuration Examples for ISG Access for PPP Sessions

Configuring ISG Access for PPP Sessions Example

The following example shows the configuration of an ISG policy that provides services to PPP subscribers. This example configures ISG to perform the following actions:

- PPP local termination

ISG will provide local termination by activating the service “ispa” for subscribers matching the domain “ispa”. The system will authenticate the subscriber using method-list “list1”. For local termination services, the global VRF is applied by default unless another VRF is specified in the service profile, on the interface, or in the virtual template.

- PPP authentication before forwarding

ISG will locally authenticate subscribers matching domain “ispb” before forwarding the sessions to an LNS. (Sessions are forwarded to an LNS because service policy map “ispb” specifies a VPDN group). The system will authenticate the subscribers using method-list “list2”.

- PPP forwarding without local authentication

ISG will forward sessions to an LNS without local authentication for subscribers matching domain “ispc”.

- PPP domain exclusion

ISG will deny service to and disconnect the session for subscribers matching domain “ispd”.

- PPP domain-based service activation

For subscribers matching all other domains, ISG will activate a service that has the same name as the specified domain.

Configure control class maps, which define the conditions that must be met before a control policy rule will be executed.

```
class-map type control match-all PPP_SESSION
  match protocol ppp

class-map type control match-all NAS_PORT_CONDITION
  class type control match identifier name PPP_SESSION
  less-than identifier nas-port type atm vpi 200 vci 100
class-map type control match-all ISPA
  match unauthenticated-domain ispa

class-map type control match-all ISPB
  match unauthenticated-domain ispb

class-map type control match-all ISPC
  match unauthenticated-domain ispc

class-map type control match-all ISPD
  match unauthenticated-domain ispd
```

Define the top-level control policy map.

```
policy-map type control L2_ACCESS
```

Define a control policy rule that activates a forwarding service on the basis of the ATM VPI/VCI on which the call came in.

```
 class type control NAS_PORT_CONDITION event session-start
  1 service-policy type service xconnect
```

Define a control policy rule that collects the domain name from the protocol. The domain name is available from a structured user name (e.g., user@domain).

```
 class type control PPP_SESSION event session-start
  1 collect identifier unauthenticated-domain
  2 service-policy type control DOMAIN_BASED_ACCESS
```

Define the nested control policy.

```
policy-map type control DOMAIN_BASED_ACCESS
```

Define a control policy rule that provides local termination by activating the service “ispa”.

```
 class type control ISPA event session-start
  1 authenticate aaa list list1
  2 service-policy type service ispa
```

Define a control policy rule that configures the system to authenticate the subscriber locally before activating service “ispb”. The service “ispb” specifies forwarding the session to an LNS.

```
 class type control ISPB event session-start
  1 authenticate aaa list list2
  2 service-policy type service ispb
```

Define a control policy rule that activates service “ispc”, which specifies forwarding.

```
 class type control ISPC event session-start
  1 service-policy type service ispc
```

Define a control policy rule that results in session disconnection for subscribers that match service “ispd”.

```
 class type control ISPD event session-start
  service disconnect
```

Define a control policy rule that defines the default for all other domains, which is to activate a service having the same name as the specified domain.

```
 class type control always event session-start
    service-policy type service identifier unauthenticated-domain
```

Configure the service policy maps.

```
policy-map type service xconnect
  service vpdn group 1

policy-map type service ispa
  service local
  ip vrf forwarding red

policy-map type service ispb
  service vpdn group 2

policy-map type service ispc
  service vpdn group 3
```

Apply the control policy map globally.

```
service-policy type control L2_ACCESS
```

VRF Transfer for PPP Sessions Using IPCP Renegotiation Example

The following example shows a configuration that uses PPPoE to establish a session, and the RADIUS service profile that is created to associate the VRF. In this example, when a PPP session initially comes up, it belongs to the default routing table, and the IP address is assigned from the default IP address pool “DEF-POOL”. When the subscriber selects the “ISP-RED” service, ISG downloads the “ISP-RED” service profile and applies it to the session. The PPP session is then transferred to VRF “RED”. IPCP renegotiation occurs between the client device and the ISG device, and the subscriber is assigned a new IP address from the pool “POOL-RED”.

```
ip vrf RED
 rd 1:1
interface Loopback0
 ip address 10.0.0.1 255.255.255.0
interface Loopback1
 ip address 10.0.1.0 255.255.255.0
 ip vrf forwarding RED
!
interface Ethernet0/0
  pppoe enable
interface Virtual-Template1
 ip unnumbered Loopback0
 service-policy control RULE2
 peer default ip address pool DEF-POOL
 ppp authentication chap
ip local pool DEF-POOL 172.16.5.1 172.16.5.250
ip local pool POOL-RED 172.20.5.1 172.20.5.250
```

Service Profile for ISP RED

```
Cisco-AVpair = ip:vrf-id=RED
Cisco-AVpair = "ip:ip-unnumbered=loopback 1"
Cisco-AVpair = ip:addr-pool=POOL-RED
Cisco-AVpair = subscriber:sg-service-type=primary
Cisco-AVpair = subscriber:sg-service-group=RED-GROUP
Cisco-SSG-Service-Info = IPPPOE-RED
Cisco-SSG-Service-Info = R10.1.1.0;255.255.255.0
Framed-Protocol = PPP
Service-Type = Framed
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	The "Authentication" section in the *Cisco IOS XE Security Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" section in the *Cisco IOS XE Security Command Reference*
PPP configuration tasks	The “PPP Configuration﷯? section in the *Cisco IOS XE Dial Services Configuration Guide*
PPP commands	*Cisco IOS XE Dial Services Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/public/support/tac/home.shtml

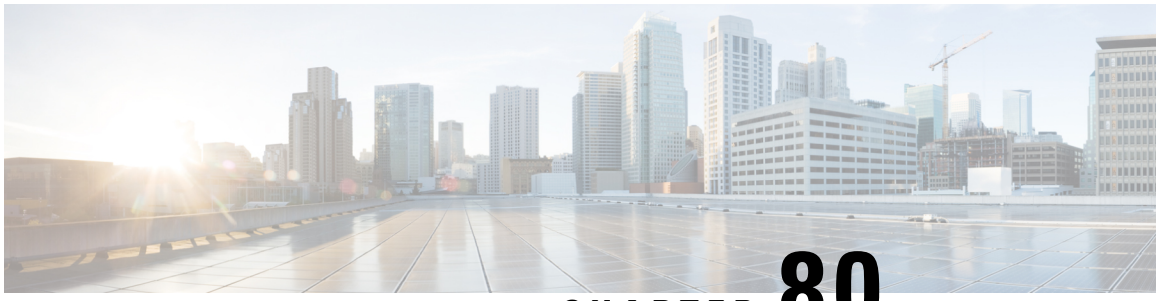
Feature Information for ISG Access for PPP Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 102: Feature Information for ISG Layer 2 Access

Feature Name	Releases	Feature Configuration Information
ISG:Session: Creation: P2P Session (PPPoE, PPPoXoX)	Cisco IOS XE Release 2.2	The ISG session is the primary context to which services and policies are associated across specific data flows. Point-to-point (P2P) sessions are established through a signaling protocol. ISG handles many variants of P2P encapsulation, such as PPP, PPPoE and PPPoA.



CHAPTER 80

Configuring ISG Access for IP Subscriber Sessions

Intelligent Services Gateway (ISG) provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports IP sessions for subscribers who connect to ISG from Layer 2 or routed Layer 3 access networks. This module describes how to configure ISG to bring up IP subscriber sessions, manage subscriber IP addressing, and configure dynamic VPN selection.

Note This document assumes that network address translation (NAT) is performed on a different Layer 3 gateway other than ISG.

Prerequisites for ISG Access for IP Subscriber Sessions

- The DHCP server must support the DHCP lease protocol.
- For ISG to use DHCP to assign IP addresses, the following conditions must be met:
  - The subscriber must be Layer 2-connected.
  - ISG must be in the path of DHCP requests, serving as a DHCP server or relay.
  - Appropriate IP subnets must be configured on the subscriber interface.

Restrictions for ISG Access for IP Subscriber Sessions

IPv6 Session Restrictions

- Layer 2 connected interfaces are not supported. Only Layer 3-routed inband IPv6 sessions are supported.
- Out-of-band IPv6 sessions are not supported.
- DHCP-initiated or RADIUS proxy-initiated sessions are not supported for IPv6 sessions.
- Dual-stack sessions are not supported. A native IP session can have either an IPv4 or IPv6 address, not both.

Overlapping IP Address Restrictions

- Overlapping IP addresses in the same virtual routing and forwarding (VRF) instance are not supported.
- Overlapping IP subscribers in different VRFs on the same interface are not supported for static and routed IP subscriber sessions. In contrast, overlapping IP subscribers in different VRFs on the same interface are supported for Layer 2-connected DHCP subscriber sessions.

IP Subnet Session Restrictions

IP subnet sessions are not supported on an interface configured with the **ip subscriber l2-connected** command. IP subnet sessions are supported only when the **ip subscriber routed** command is configured on the interface.

ISG DHCP Restrictions

ISG cannot relay DHCP requests when a Layer 3 DHCP relay agent is between an ISG device and subscriber devices.

Dynamic VPN Selection Restrictions

- Dynamic VPN selection is not supported for IP interface sessions, IP subnet sessions, and subscribers connecting on nonglobal VRF interfaces.
- Dynamic VPN selection is not supported for subscribers with a static VPN configuration on the access interface.
- Dynamic VPN selection with address reassignment is not supported for routed IP subscriber sessions that are initiated by DHCP. The IP addresses of routed IP subscribers must be routable in the access network. Because ISP- or VRF-owned private addresses could overlap or be unroutable in the network between subscribers and an ISG device, IP addresses cannot be addressed to subscribers in such networks.
- IP interface sessions do not support dynamic VRF; only static VRF is supported. If an interface is configured with the **ip subscriber interface** command, dynamic VRF through a RADIUS vendor-specific attributes (VSA) is not supported; only static VRF is supported.
- Traffic from locally imported VRF routes is not supported for subscribers. From subscriber side, VRF transfer works fine.

General IP Session Restrictions

- Virtual Fragment Reassembly (VFR) configuration is not supported on the virtual-template interface.
- IP subscriber sessions are not supported on ambiguous IEEE 802.1QinQ or IEEE 802.1Q (Dot1Q) subinterfaces.
- IP subscriber sessions are not supported on interfaces that receive Multiprotocol Label Switching (MPLS) packets.
- Modular quality of service (QoS) CLI (MQC) shaping and queueing is supported in the egress direction in the default class for IP subscriber sessions.
- Configuring features on static IP sessions is not supported.
- ISG IP subscriber functionality is not supported on the following types of access interfaces:
  - Layer 2 Tunnel Protocol (L2TP)
  - PPP (virtual template)
- Interface statistics are not generated for ISG multiservice interfaces.
- Stateful switchover (SSO) and In Service Software Upgrade (ISSU) are not supported for DHCP IP sessions (where ISG serves as a relay or server). Upon switchover, a DHCP IP session must be restarted when the session becomes active again.
- The following subscriber features are not supported for Internet Protocol over Ethernet (IPoE) sessions:
  - Per-session firewall
  - Per-session NAT
  - Per-session netflow
  - Per-session network-based application recognition (NBAR)
  - Per-session multicast
  - Per-session policy-based routing (PBR)
- The following PPP session features are not supported for IP sessions:
  - Packet of Disconnect (PoD)
  - Session limit per system, VLAN, or MAC

Note IP Sessions over Gigabit EtherChannel (IPoGEC) and IP Sessions over EoGRE tunnels are supported starting from Cisco IOS XE Release 3.9S. For more information, see IP Sessions Over Gigabit EtherChannel Chapter of the *Intelligent Wireless Access Gateway Configuration Guide*.

Note Network Address Translation (NAT) configuration is supported on the access side of ISG starting from Cisco IOS XE Release 3.12S. For more information, see IP Sessions Over Gigabit EtherChannel Chapter of the *Intelligent Wireless Access Gateway Configuration Guide*.

Multiservice Interface Restrictions

- IP interface features such as QoS and access lists are not supported on multiservice interfaces.
- Only one multiservice interface can belong to a single VRF. For example, the following configuration will not work:

```
interface multiservice 1
 ip vrf forwarding VRF_A
!
interface multiservice 2
 ip vrf forwarding VRF_A
```

Information About ISG Access for IP Subscriber Sessions

Types of IP Subscriber Sessions

ISG supports the types of IP subscriber sessions described in the following sections:

IP Sessions

An IP session includes all the traffic that is associated with a single subscriber IP address. If the IP address is not unique to the system, other distinguishing characteristics such as a VRF or a MAC address form part of the identity of the session. ISG can be configured to create IP sessions when it receives DHCP packets, packets with unclassified IP or MAC addresses, or RADIUS packets. See the "IP Subscriber Session Initiation" section for more information.

IP sessions may be hosted for a connected subscriber device (one routing hop from the ISG) or a subscriber device that is more than one hop from the gateway.

IP Interface Sessions

An IP interface session includes all the IP traffic that is received on a specific physical or virtual interface. IP interface sessions are created when the IP interface session commands are entered. The session remains continuous even when the interface is shut down. By default, IP interface sessions come up in the unauthenticated state with full network access.

IP interface sessions can be used in situations where a subscriber is represented by an interface (with the exception of PPP) and communicates using more than one IP address. For example, a subscriber using a routed bridge encapsulation (RBE) access might have a dedicated ATM virtual circuit (VC) to home customer premises equipment (CPE) that is hosting a number of PCs.

IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, that is ISG features and functionality are applied to the subnet traffic as an aggregate.

IP subnet sessions are supported for routed IP subscriber traffic.

IP subnet sessions are created in the same way as IP sessions, except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Note Where an ingress interface maps to a single subnet, the subnet might be accommodated with an IP interface session. However, if an ISG device is more than one hop away from a subscriber, and multiple subnets could be accessible through the same interface, IP subnet sessions may be defined to distinguish the traffic and apply appropriate edge functionality to each subnet.

Coexistence of Multicast and IP Sessions

The ISG Session Multicast Coexistence feature introduces the ability to host all subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco ASR 1000 Series Aggregation routers. ISG IP sessions are supported on nonaccess-type subinterfaces. For an existing session or even when no session exists, this support helps multicast traffic to pass through the interfaces that are configured for IP sessions in both upstream and downstream directions without creating a session.

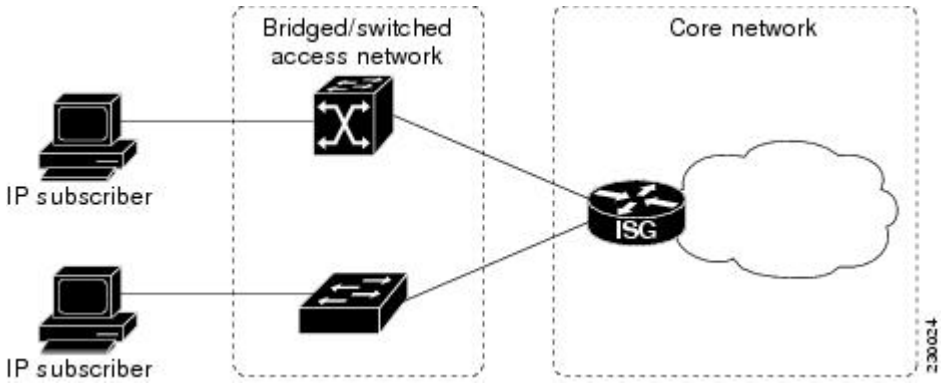
IP Subscriber Connectivity

IP subscribers connect to ISG through either Layer 2-connected access networks or routed access networks. The following sections describe these types of IP subscriber connectivity:

Layer 2-Connected Access Networks

Layer 2-connected subscribers are either directly attached to the physical interfaces of ISG or connected to ISG through a Layer 2 access network, such as a bridged or a switched network. Layer 3 forwarding is either absent or not used to direct subscriber traffic in the Layer 2 access network. IP addresses of the subscribers may or may not be on the same subnet as the Layer 2-connected physical interfaces. The figure below shows an example of a Layer 2-connected access network.

Figure 56: Layer 2-Connected Access Network

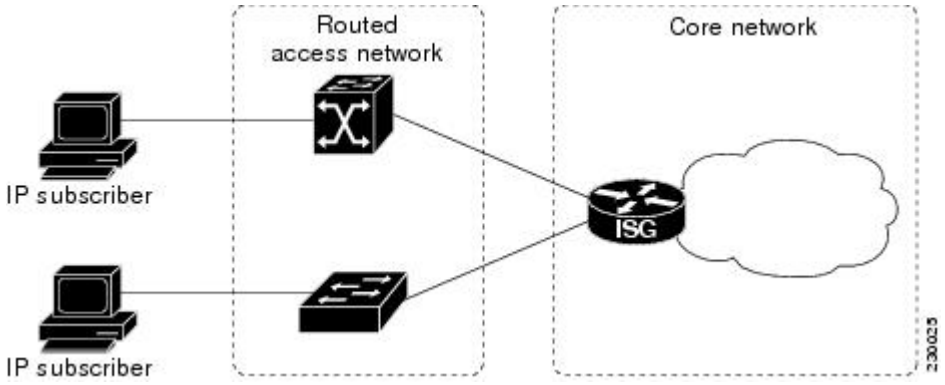


Roaming can be configured on Layer 2-connected IP subscriber sessions by using the **ip subscriber l2-roaming** command. When a Layer 2-connected IP subscriber tries to establish a session with an existing MAC address and a new IP address on an interface that is different from the one that is running the current session, ISG terminates the existing session and creates a new session with a new MAC address-IP address pair. When the subscriber tries to establish a session with an existing MAC address and a new IP address on the same interface that is running the current session, ISG blocks the new session.

Routed Access Networks

For routed access networks, subscriber traffic is routed through a Layer 3 access network with at least one transit router before reaching the ISG. IP addresses of the subscribers are at least routable in the Layer 3 access network. Layer 3 access networks contain a single routing domain and therefore, do not support overlapping IP addresses. The figure below shows an example of a routed access network.

Figure 57: Routed Access Network



IP Subscriber Session Initiation

ISG can be configured to allow one or more of the following events to signal the start of an IP session or IP subnet session on an interface:

- DHCP DISCOVER packet— If the following conditions are met, an IP session is created after ISG receives a DHCP DISCOVER packet:
  - ISG serves as a DHCP relay or a server for new IP address assignments.

- Subscribers are configured for DHCP.
- The DHCP DISCOVER packet is the first DHCP request received from the subscriber.
- Source IP address is unclassified— For routed IP subscribers, a new IP session is triggered when an IP packet with an unclassified source IP address (an IP session does not yet exist for that IP address) is received.

- Unclassified source MAC address— For Layer 2-connected IP subscribers, a new IP session is triggered when an IP packet with an unclassified source MAC address (which means that an IP session does not yet exist for that MAC address) is received.
- RADIUS Access-Request packet— For routed or Layer 2-connected access, a new IP session is triggered by the appearance of a RADIUS Access-Request packet when ISG is serving as a RADIUS proxy.

IP Subscriber Addressing

The following sections provide information about how ISG handles IP addressing for IP subscribers:

Methods of ISG Subscriber IP Address Assignment

IP subscribers either have IP addresses configured statically or obtain IP addresses dynamically through some network protocol that has the ability to assign IP addresses. For a subscriber to be routable within a given IP service domain, the subscriber must present a domain-specific IP address to the network. If a subscriber transfers between IP service domains (including any private domain managed by the access provider), the IP address presented to the network must change to reflect the new domain.

The following sections describe the methods of IP address assignment that ISG supports for each type of Layer 3 session:

IP Interface Sessions

For IP interface sessions, ISG is not involved in (or aware of) the assignment of subscriber IP addresses.

IP Sessions

For IP sessions, ISG supports the following methods of IP address assignment:

- Static IP addresses—If a subscriber's static IP address is configured correctly for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.
- DHCP—If DHCP is being used to assign IP addresses, and the IP address that is assigned by DHCP is correct for the service domain, ISG does not have to be involved in the assignment of an IP address for the subscriber.

  If the IP address that is assigned by DHCP is not correct for the service domain or if the domain changes because of a VRF transfer, ISG can be configured to influence the DHCP IP address assignment.

  The following conditions must be met for ISG to influence DHCP IP address assignment:

  - The subscriber must be Layer 2-connected.
  - The ISG device must be in the path of DHCP requests by serving as a DHCP server or relay.
  - Subscribers must not have statically configured IP addresses.

  For deployments that support it, DHCP is the recommended method of IP address assignment.

IP Subnet Sessions

For IP subnet sessions, the IP subnet is specified in the user profile.

Public and Private IP Addresses

An IP address falls in either the public or the private IP address category, irrespective of the method used to assign the IP address to the IP subscriber. If an IP subscriber is assigned a private IP address and the subscriber has to reach the Internet, a Layer 3 gateway, such as an ISG or a firewall, that is present between the subscriber and the Internet must perform Network Address Translation (NAT) for the subscriber's private IP address.

When the access network is a Layer 2-connected network, a subscriber IP address can be either native or foreign to an access interface. A native subscriber IP address belongs to the subnet provisioned on the access interface. A foreign subscriber IP address does not belong to the subnet provisioned on the access interface. A foreign subscriber IP address could result when a retail ISP assigns an IP address to the IP subscriber from its own IP address allotment, which is different from the wholesale ISPs, or when an IP subscriber with a static IP address that is native in the home access network roams to a foreign access network. To support IP subscribers with foreign IP addresses, ISG must be able to respond to Address Resolution Protocol (ARP) requests that originate from foreign IP addresses with a MAC address of the ISG itself. Because the access network is Layer 2-connected, ISG maintains an adjacency to every subscriber.

When the access network is a routed network, a subscriber IP address must be routable in the access network; otherwise, subscriber traffic will never be able to reach ISG. ISG may not have an adjacency for each subscriber in this case, but has an adjacency of the next hop towards a subscriber. The next hop is determined by the routing process on ISG.

Overlapping IP Addresses

When an access network is deployed without VPN capability, the IP address space in the access network is shared among all IP subscribers. When the IP addresses are assigned dynamically, care must be taken to ensure that these addresses do not overlap. When overlapping IP addresses are assigned to IP subscribers intentionally, the access network should use a Layer 2 separation mechanism to differentiate the IP address spaces. For example, the access network may put each IP address space in a different VLAN.

When the access network serves both local IP subscribers and roaming users, the static private IP address of a roaming subscriber may overlap the native private IP address of another subscriber. For example, a public wireless hotspot that generally assigns dynamic IP addresses may provide access to occasional roaming users with statically configured IP addresses. To support this special overlapping condition, all IP subscribers must be in a Layer 2-connected access network in which overlapping MAC addresses do not exist. In this case, IP subscribers can be distinguished using MAC addresses.

ISG Subscriber IP Address Assignment Using DHCP

When ISG is in the path of DHCP requests (as either a DHCP server or a DHCP relay), ISG can influence the IP address pool and the DHCP server that are used to assign subscriber IP addresses. To enable ISG to influence the IP addresses assigned to subscribers, associate a DHCP address pool class with an address domain. The DHCP address pool class must also be configured in a service policy map, service profile, or user profile that is associated with a subscriber. When a DHCP request is received from a subscriber, DHCP uses the address pool class that is associated with the subscriber to determine which DHCP address pool should be used to service the request. As a result, on a per-request basis, an IP address is either provided by the local DHCP server or relayed to a remote DHCP server that is defined in the selected pool.

IP Subscriber Identity

IP subscriber identity is closely related to IP session initiation because ISG must uniquely identify an IP subscriber at the time that it creates an IP session. However, the need to identify an IP subscriber goes beyond the session initiation phase. The following sections describe how ISG uniquely identifies IP subscribers:

Routed IP Subscriber Identity

By definition, subscriber IP addresses are at least routable in the access network. If the access network is a routed network, subscriber IP addresses can be used to uniquely identify IP subscribers.

When using a subscriber IP address as the identifier, ISG assumes that the subscriber IP address is unique. If the access network is deployed with Layer 3 load balancing, redundancy, or asymmetric routing, ISG also assumes that IP traffic from the same IP subscriber may arrive at different access interfaces. To support this type of deployment, ISG assumes a single IP address space for all access interfaces connecting to the same access network.

If there is a requirement to support several IP address spaces over a single physical access network, the access network must use some Layer 2 encapsulation to create a separate logical access network for each IP address space. In this case, ISG can still have a single IP address space for all the logical access interfaces that connect to a logical access network.

When subscriber IP addresses are private IP addresses, the access network must be able to route such subscriber traffic. If the subscriber traffic is destined for the Internet, NAT must be performed.

For routed IP subscribers, the subscriber IP address serves as the key for an IP session. ISG associates IP traffic with an IP session as follows:

- In the upstream direction, the source IP address of an IP packet is used to identify the IP session. The source IP address is the subscriber IP address.
- In the downstream direction, the destination IP address of an IP packet is used to identify the IP session. The destination IP address is the subscriber IP address.

If the IP subscriber is a VPN user, the subscriber IP address must be routable in both the global routing table and the VPN routing table on ISG.

For an IP subnet subscriber, a subscriber IP address is defined as an IP prefix address instead of a /32 IP host address. This IP prefix covers a range of IP addresses used by end users but represents a single logical IP subscriber for ISG. In this deployment, all end users share the same connectivity and services provided by ISG.

To normalize the classification of IP subscribers that have different network masks, ISG uses the network mask in conjunction with the subscriber IP address for routed IP subscribers.

MAC Address as Secondary Identity

You must configure the **collect identifier mac-address** command at the start of a session. This instructs the ISG devices to store the MAC address as part of the session identifiers. For routed IP subscriber sessions, the MAC address is collected from the DHCP server using the DHCP lease Query Protocol. For information about configuring the command, see the “Configuring ISG Control Policies” module.

DHCP Lease Query Support

The DHCP lease query message is a DHCP message type transmitted from a DHCP relay agent to a DHCP server. A DHCP lease query-aware relay agent sends the location of an IP endpoint to the DHCP lease query message.

The DHCP lease query transaction is a DHCP transaction with special message types that enable clients to query DHCP servers regarding the owner and the lease expiration time of an IP address.

Layer 2-Connected IP Subscriber Identity

A Layer 2-connected access network can provide IP connectivity to IP subscribers with native IP addresses and foreign and overlapping IP addresses. Because subscriber IP addresses might not be unique in such an access network, ISG uses the subscriber MAC address to identify Layer 2-connected IP subscribers.

Traffic that comes from IP subscribers with private or overlapping IP addresses and that is destined to the Internet is subject to NAT.

For Layer 2-connected IP subscribers, both the subscriber MAC address (unique within a VLAN) and the IP address, serve as keys for the IP session and are used in the following directions:

- In the upstream direction, the VLAN ID and source MAC address of an IP packet are used to identify the IP session.
- In the downstream direction, the destination IP address and the VLAN ID of an IP packet are used to identify the IP subscriber context.

VPN Connectivity and Services for IP Subscribers

Subscriber VPN Membership

Based on the deployment requirements, an IP subscriber may or may not have the VPN service. If an IP subscriber does have the VPN service, the subscriber may belong to only one VPN domain at any time. An IP subscriber is associated with a VPN domain in one of the following ways:

- Static VPN assignment—The VPN IP subscriber belongs to a static VPN domain. Whenever the IP subscriber connects to ISG, the IP subscriber is placed in the preassigned VPN domain.
- Dynamic VPN selection—The VPN IP subscriber can choose and switch among different VPN domains through dynamic service login. Whenever a new VPN domain is selected, VPN services of the current VPN domain must be removed before VPN services of the new VPN domain can be applied to the IP subscriber.

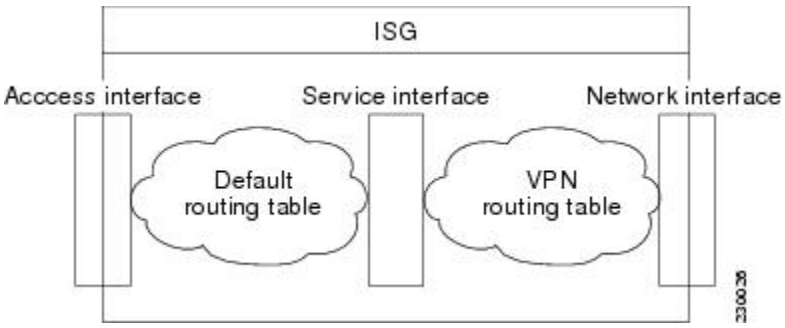
Dynamic VPN selection can be initiated through automatic service login, where the virtual routing and forwarding (VRF) instance is downloaded and applied to the subscriber session at the start of a session. Dynamic VPN selection can also be initiated through subscriber service selection at a web portal, where the subscriber is transferred to the VRF that corresponds to the selected service.

Multiservice Interface Model

For a subscriber without a static VPN configuration, a multiservice interface must be configured on the ISG device to map the IP session to a VRF instance. The multiservice interface represents a boundary between a VPN routing domain and the default routing domain. When an IP subscriber is associated with several routing domains throughout the duration of a connection, multiservice interfaces serve as demarcation points for the

IP subscriber to switch from one VPN domain to another VPN domain. One multiservice interface must be configured for each VPN routing domain. The figure below illustrates the multiservice interface model.

Figure 58: Multiservice Interface Model



VPN Addressing

When a subscriber session is transferred from one VPN domain to another, the session enters a new addressing domain that may or may not overlap the previous domain of the subscriber. The network-facing address of the subscriber must be altered accordingly, so that packets can be correctly routed back from within the service domain.

A VRF transfer is necessary when a identity of the subscriber and subscribed services cannot be determined without interaction with a web portal. A local routing context is required, at least initially, so that IP packets may be routed to and from the portal server. After the portal-based service selection, the subscriber has to be transferred into the VRF that is associated with the selected service domain. After the VRF transfer, the subscriber must also receive an address that is routable in this new domain.

If ISG is adjacent to the subscriber device and serves as a DHCP relay or server, DHCP can be used to assign domain-specific addresses to subscribers.

To support VRF transfers, DHCP should be configured with short initial leases. This is because existing subscriber addresses can be altered only after the current lease has expired. Subscribers will not have access to the selected domain before the next DHCP renew request is received. Using short initial lease times minimizes the interval between a VRF change and a DHCP renewal. If long lease times are used, an out-of-band method of initiating IP address change should be implemented.

When DHCP can be used to assign a new address at the subscriber device, subnet-based VRF selection can be used to bring about the transfer. Subnet-based VRF selection (also known as *VRF autoclassify*) is a feature that selects the VRF at the ingress port on the basis of the source IP subnet address.

Service providers and organizations have public IP address blocks allocated to them that are not overlapping by nature. Therefore, when they are assigned public IP addresses, VPN IP subscribers have no overlapping IP addresses. When VPN IP subscribers of different VPN domains have private IP addresses assigned, they are likely to have overlapping addresses in the access network.

An access network is a single IP address space when there is no Layer 2 encapsulation separating VPN IP subscribers of different VPN domains. Therefore, ISG must be able to handle overlapping IP addresses when deploying VPN IP subscribers. IP connectivity for VPN IP subscribers with overlapping IP addresses is possible only when they are connected to ISG through a Layer 2-connected access network.

VPN IP Subscriber Identity

ISG identifies VPN IP subscribers in the same way that it identifies non-VPN IP subscribers. Upstream IP traffic is defined as the subscriber IP traffic traveling from the access network to the VPN (overlaid on top of the service provider core network). Downstream IP traffic is defined as the subscriber IP traffic traveling from the VPN to the access network.

Service Model for VRF Transfers

A *primary* service contains a network-forwarding policy (such as a VRF) in its service definition. Only one primary service at a time can be activated for a session. A secondary service is any service that does not contain a network-forwarding policy.

When a subscriber for whom a primary service has already been activated tries to select another primary service, ISG deactivates all current services (including the current primary service) and activates the new primary service, and hence, switches the VRF.

When a subscriber for whom a primary service has already been activated tries to select a secondary service, the action taken by ISG depends on whether the secondary service is part of a service group. A service group is a grouping of services that may be simultaneously active for a given session. Typically, a *service group* includes one primary service and one or more secondary services. The table below describes the action that ISG will take when a subscriber selects a secondary service.

Table 103: ISG Activation Policy for Secondary Services

Primary Service Characteristics	Secondary Service Characteristics	Resulting Behavior at ISG
Primary service with no service group attribute	Secondary service with service group	Do not bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.
Primary service with service group attribute	Secondary service with different service group	Do not bring up the secondary service.
	Secondary service with same service group	Bring up the secondary service.
	Secondary service with no service group	Bring up the secondary service.

Benefits of Dynamic VPN Selection

The need for switching of a subscriber session between routing and forwarding domains (also called *network services*) occurs frequently in markets where equal access networking must be supported. Equal access networking is often mandated by regulatory rules stating that an access provider should allow service providers equal access to a retail subscriber network. ISG dynamic VPN selection facilitates equal access networking by allowing subscribers to transfer between network services.

IP Session Termination

An IP session may be terminated in one of the following ways:

- DHCP lease expiry or DHCP release from client—If DHCP is used to detect a new session, its departure may also be signaled by a DHCP event.

- Application stop—The **application stop** command is typically used to terminate a session when a subscriber initiates an account logout from a web portal. An application stop may also result from the actions of an administrator, such as action taken in response to rogue behavior from a subscriber.
- Idle timeout and session timeout—Idle timeouts and session timeouts can be used to detect or impose termination of an IP session.
- Control policy—A control policy containing the service disconnect action can be used to terminate a session.

IP Session Recovery for DHCP-Initiated IP Sessions

When an IP session is terminated (for example, by account logoff or session timeout) or lost (for example, by router reload), the client may continue to hold an unexpired DHCP lease. When the client continues to hold an unexpired DHCP lease, ISG performs a session restart to prevent the client's IP connection from being nonfunctional until the DHCP lease expires. A control policy can be configured to define the actions that ISG performs when the session restart event occurs. If a policy is not defined, a default policy takes effect. The default policy causes ISG to disconnect the session after 60 seconds after a session restart and is the equivalent of the following configuration:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

This default policy appears in the output of the **show subscriber policy rules** command, as follows:

```
Rule: internal-rule-session-restart
 Class-map: always event session-restart
  Action: 1 service disconnect delay 60
  Executed: 0
```

Default Services for IP Subscriber Sessions

New IP sessions may require a default service to allow subsequent subscriber packets to be processed appropriately; for example, to permit or force TCP packets to a captive portal where menu-driven authentication and service selection can be performed. A default service policy map or service profile may be configured for IP sessions to redirect traffic, enable port-bundle host-key functionality for session identification, or enable transparent autologin. A default service might also include a network service, which allows subscribers to access a web portal for authentication and service selection.

How to Configure ISG for IP Subscriber Sessions

Creating ISG Sessions for IP Subscribers

An Intelligent Services Gateway (ISG) device creates IP sessions for IP traffic on subscriber-side interfaces. The tasks in the following sections enable IP sessions and indicate how sessions are identified:

Creating IP Subscriber Sessions for Routed ISG Subscribers

IP subscribers that are routed through a Layer 3 access network with at least one transit router before reaching ISG are known as routed IP subscribers. Perform this task to configure ISG to create IP sessions for routed IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address** [**ipv4** | [**ipv6**] [**list** *list-name*]]}
6. **passthru downstream ipv6**
7. **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** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber routed** **Example:** `Device(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode.
Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified ip-address** [**ipv4** | [**ipv6**] [**list** *list-name*]]} **Example:** `Device(config-subscriber)# initiator unclassified ip-address`	Enables ISG to create an IP subscriber session upon receipt of the specified packet type. • Enter this command more than once to specify more than one method of IP session initiation. **Note** If the ISG device serves as either a DHCP relay or a DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions on receiving DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip-address** or **initiator unclassified mac-address** command.

	Command or Action	Purpose
Step 6	**passthru downstream ipv6** **Example:** `Device(config-subscriber)# passthru downstream ipv6`	(Optional) Allows IPv6 downstream traffic from the ISG interface to pass through without a subscriber session.
Step 7	**end** **Example:** `Device(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers

Layer 2-connected subscribers are either directly attached to the physical interfaces of an ISG or connected to an ISG through a Layer 2 access network, such as a bridged network or a switched network. Perform this task to configure ISG to create IP sessions for Layer 2-connected IP subscribers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber l2-connected**
5. **initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**}
6. **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** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber l2-connected** **Example:**	Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode.

	Command or Action	Purpose
	`Device(config-if)# ip subscriber l2-connected`	**Note** We recommended that you configure IP sessions for Layer 2-connected subscribers using the **ip subscriber l2-connected** command. However, you could also use the **ip subscriber routed** command if subscriber IP addresses are routable in the access domain.
Step 5	**initiator** {**dhcp** [**class-aware**] | **radius-proxy** | **unclassified mac-address**} **Example:** `Device(config-subscriber)# initiator unclassified mac-address`	Configures ISG to create an IP subscriber session upon receipt of the specified packet type. • Enter this command more than once to specify more than one method of IP session initiation. **Note** If the ISG device serves as either a DHCP relay or a DHCP server in the assignment of client IP addresses, ISG must be configured to initiate IP sessions upon receipt of DHCP DISCOVER packets. In other words, the **initiator dhcp** command must be configured instead of the **initiator unclassified ip-address** or **initiator unclassified mac-address** command.
Step 6	**end** **Example:** `Device(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating ISG IP Interface Sessions

An ISG IP interface session encompasses all IP packets that cross the specified interface or subinterface. Perform this task to create an ISG IP interface session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*[**.** *subinterface-number*]
4. **ip subscriber interface**
5. **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	**interface** *type number*[**.** *subinterface-number*] **Example:** `Device(config)# interface GigabitEthernet 0/0/0.1`	Specifies an interface or subinterface and enters interface or subinterface configuration mode.
Step 4	**ip subscriber interface** **Example:** `Device(config-subif)# ip subscriber interface`	Specifies the type of IP subscriber to be hosted on the interface. **Note** The **ip subscriber interface** command cannot be configured if the **service-policy input** or **service-policy output** command is already configured on the interface; these commands are mutually exclusive.
Step 5	**end** **Example:** `Device(config-subif)# end`	(Optional) Returns to privileged EXEC mode.

Creating ISG Static Sessions

An Intelligent Services Gateway (ISG) static session enables you to configure static IP sessions by configuring a group of server addresses. Perform the following task to create ISG static sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ip source** *ip-address* {**mac** *mac-address* | **mask** *subnet-mask*}
5. **exit**
6. **interface** *type number*
7. **ip subscriber** {**l2-connected** | **routed**}
8. **initiator static ip subscriber list** *list-name*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip subscriber list** *list-name* **Example:** `Device(config)# ip subscriber list mylist`	Specifies the IP subscriber list name and enters server list configuration mode.
Step 4	**ip source** *ip-address* {**mac** *mac-address* | **mask** *subnet-mask*} **Example:** `Device(config-server-list)# ip source 209.165.200.225 mac 0.7.f`	Specifies the static server IP address and MAC address (in case of Layer 2-connected subscribers) or subnet mask (in the case of routed interfaces).
Step 5	**exit** **Example:** `Device(config-server-list)# exit`	Exits server list configuration mode and returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 2/0/0`	Specifies an interface and enters interface configuration mode.
Step 7	**ip subscriber** {**l2-connected** | **routed**} **Example:** `Device(config-if)# ip subscriber l2-connected`	Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode. **Note** IP sessions for Layer 2-connected subscribers should be configured using the **ip subscriber l2-connected** command. However, the **ip subscriber routed** command can also be used if subscriber IP addresses are routable in the access domain.
Step 8	**initiator static ip subscriber list** *list-name* **Example:** `Device(config-subscriber)# initiator static ip subscriber list mylist`	Creates an IP subscriber session with the packet type as static and attaches the session to the list.
Step 9	**end** **Example:** `Device(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.

Creating ISG IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet

session is configured, ISG treats the subnet as a single subscriber, which means that ISG features and functionality are applied to the subnet traffic as an aggregate. Perform this task to create an IP subnet session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator unclassified ip-address** [**ipv4** | [**ipv6**] [**list** *list-name*]]
6. **end**
7. Add the Framed-IP-Netmask attribute to the service or user profile.

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** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber routed** **Example:** `Device(config-if)# ip subscriber routed`	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.
Step 5	**initiator unclassified ip-address** [**ipv4**	[**ipv6**] [**list** *list-name*]] **Example:** `Device(config-subscriber)# initiator unclassified ip-address`	Configures ISG to create an IP subscriber session when an IP packet with an unclassified IP source address is received.
Step 6	**end** **Example:** `Device(config-subscriber)# end`	(Optional) Returns to privileged EXEC mode.
Step 7	Add the Framed-IP-Netmask attribute to the service or user profile.	Enables an IP subnet session for the subscriber. • When a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based

	Command or Action	Purpose
		session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Configuring IP Session Recovery for DHCP-Initiated IP Sessions

Perform this task to configure Intelligent Services Gateway (ISG) to take specific actions after the recovery of an IP session when ISG has terminated or reloaded the session. This task applies to DHCP-initiated IP sessions only.

If a policy for session recovery is not configured, ISG applies the following default policy:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **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	**policy-map type control** *policy-map-name* **Example:** `Device(config)# policy-map type control MY-POLICY`	Creates or modifies a control policy map, which is used to define a control policy, and enters control policy-map configuration mode.

	Command or Action	Purpose
Step 4	**class type control** {*control-class-name* | **always**} **event session-restart** **Example:** `Device(config-control-policymap)# class type control always event session-restart`	Specifies a control class that is evaluated when the session-restart event occurs and enters policy-map class control configuration mode. • A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.
Step 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **Example:** `Device(config-control-policymap-class-control)# 1 authorize identifier source-ip-address`	(Optional) Initiates a request for authorization on the basis of the specified identifier.
Step 6	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}} **Example:** `Device(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT`	(Optional) Activates an ISG service. • Specifying an identifier instead of a service name activates a service that has the same name as the specified identifier.
Step 7	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Device(config-control-policymap-class-control)# 1 set-timer TIMERA 5`	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy expiry.
Step 8	**end** **Example:** `Device(config-control-policymap-class-control)# end`	(Optional) Returns to privileged EXEC mode.

Verifying ISG IP Subscriber Sessions

Perform this task to verify IP subscriber session configuration and creation. The **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

3. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
4. **show platform isg session-count** {**all** | *slot*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier*	**uid** *session-id*	**username** *name*] **Example:** `Device# show subscriber session detailed`	Displays information about ISG policies and features for subscriber sessions.
Step 3	**show ip subscriber** [**mac** *mac-address*	[**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**]	**interface** *interface-name* [**detail**	**statistics**]	**ip** *ip-address*	**static list** *listname*	**statistics** {**arp**	**dangling**}]] **Example:** `Device# show ip subscriber ip 10.10.10.10`	Displays information about ISG IP subscriber sessions.
Step 4	**show platform isg session-count** {**all**	*slot*} **Example:** `Device# show platform isg session-count all`	Displays the number of active ISG subscriber sessions by line card.

Clearing ISG IP Subscriber Sessions

SUMMARY STEPS

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]

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	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** `Device# show ip subscriber ip 10.10.10.10`	(Optional) Displays information about ISG IP subscriber sessions.
Step 3	**clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **Example:** `Device# clear ip subscriber ip 10.10.10.10`	Clears ISG IP subscriber sessions.

Troubleshooting ISG IP Subscriber Sessions

Use the following commands to troubleshoot ISG IP subscriber sessions. You can use the **debug** commands in any order.

SUMMARY STEPS

1. **enable**
2. **debug ip subscriber packet**
3. **debug condition username** *username*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip subscriber packet** **Example:** `Device# debug ip subscriber packet`	Enables ISG IP subscriber session debugging.
Step 3	**debug condition username** *username* **Example:** `Device# debug condition username user1`	Filters debugging output for certain debug commands on the basis of specified conditions.

Assigning ISG Subscriber IP Addresses by Using DHCP

Configure DHCP support in your network before performing the tasks in this section.

Configuring an ISG Interface for Dynamic DHCP Class Association

Perform this task to enable ISG to influence the assignment of IP addresses to subscribers on the interface by providing the local DHCP component with a class name. The class name refers to a class configured using the **ip dhcp pool** command and can reference a pool of addresses or a relay destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** [**l2-connected** | **routed**]
6. **initiator dhcp class-aware**
7. **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** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Device(config-if)# ip address 10.1.0.1 255.255.0.0`	Sets a primary or secondary IP address for an interface.
Step 5	**ip subscriber** [**l2-connected**	**routed**] **Example:** `Device(config-if)# ip subscriber`	Enables ISG IP subscriber configuration mode.

	Command or Action	Purpose
Step 6	**initiator dhcp class-aware** **Example:** `Device(config-subscriber) initiator dhcp class-aware`	Configures ISG to create IP sessions upon receipt of DHCP DISCOVER packets. • The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
Step 7	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Configuring DHCP Server User Authentication

Perform this task to authenticate the DHCP clients on the server.

Before you begin

You need to use the ISG framework to enable DHCP server user authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*
7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp**
11. **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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new model`	Enables authentication, authorization, and accounting (AAA).
Step 4	**aaa authentication login** *list-name* **local** **Example:** `Device(config)# aaa authentication login mylist local`	Sets the AAA authentication at login.
Step 5	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool testpool`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 6	**network** *network-number mask* **Example:** `Device(dhcp-config)# network 172.16.0.0 255.240.0.0`	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco DHCP server.
Step 7	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP pool configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0`	Enters interface configuration mode.
Step 9	**ip subscriber l2-connected** **Example:** `Device(config-if)# ip subscriber l2-connected`	Configures a Layer 2-connected IP session on the interface and enters IP subscriber configuration mode.
Step 10	**initiator dhcp** **Example:** `Device(config-subscriber)# initiator dhcp`	Initiates a class for DHCP for an IP session initiated by DHCP.
Step 11	**end** **Example:** `Device(config-subscriber)# end`	Returns to privileged EXEC mode.

Configuring a DHCP Class in a Service Policy Map

Perform this task to assign a DHCP class to a service policy map. Subscribers for which this service policy map is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

Before you begin

Before configuring a DHCP class in a service policy map, you must configure a DHCP pool and the classes configured within the DHCP pool must match the DHCP classes configured in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **show policy-map type service**

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	**policy-map type service** *policy-name* **Example:** `Device(config)# policy-map type service service1`	Creates a service policy map or specifies an existing service policy map for configuration, and enters service policy-map configuration mode.
Step 4	**classname** *class-name* **Example:** `Device(config-service-policymap)# classname class1`	Associates a DHCP pool with a service policy map.
Step 5	**end** **Example:** `Device(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.
Step 6	**show policy-map type service**	(Optional) Displays the contents of all service policy maps.

	Command or Action	Purpose
	Example: `Device# show policy-map type service`	• Use this command to verify that the DHCP class is associated with the service policy map.

What to Do Next

After you have configured the DHCP address pool class in a service policy map, you may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server

Perform this task to add the vendor-specific attribute (VSA) for a DHCP class to a user profile or service profile on the AAA server. Subscribers for whom the user or service profile is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

Before configuring a DHCP class in a service profile or user profile on the AAA Server, a DHCP address pool must be configured. Classes configured within the DHCP address pool must match the DHCP address pool classes configured in the service or user profile. To associate a DHCP address pool with a service or specific subscriber, add the DHCP class attribute to the user or service profile. For example:

```
26,9,1 = "subscriber:classname=class-name "
```

After associating a DHCP address pool with a service or specific subscriber, you may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuring a DHCP Server IP Address

Perform this task to either specify which DHCP servers to use on your network or to configure the IP address of one or more DHCP servers available on the network, and to specify the DHCP Lease Query for routed IP sessions.

Note The DHCP server IP address needs to be configured for routed IP sessions if the DHCP Lease Query is performed.

Before you begin

The following prerequisites apply for this task:

- The DHCP server must support the DHCP lease protocol.
- The IP address of the phone must be assigned by DHCP address assignments.
- The traffic must be classified as Layer 3.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}}
4. **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	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}} **Example:** `Device(config)# ip dhcp-server query lease retries 3`	Configures the IP address of one or more DHCP servers available on the network, and specifies the DHCP Lease Query for routed IP sessions.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuring ISG Dynamic VPN Selection

Configuring a Multiservice Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface multiservice** *interface-number* **Example:** `Device(config)# interface multiservice 1`	Creates a multiservice interface, which enables dynamic VPN selection, and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# ip vrf forwarding vrf1`	Associates a VPN VRF with an interface or subinterface.
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 172.16.0.0 255.255.255.0`	Sets the primary IP address for an interface. • Specifies the IP address of the VPN.
Step 6	**end** **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Specifying a VRF in a Service Policy Map

VPN routing and forwarding (VRF) transfer occurs when a new primary service is activated for a session, causing the session to transfer from one VRF to another. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*
7. **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	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Device(config-service-policymap)# ip vrf forwarding vrf1`	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** `Device(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.
Step 6	**sg-service-group** *service-group-name* **Example:** `Device(config-service-policymap)# sg-service-group group1`	(Optional) Associates an ISG service with a service group. • A service group is a group of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.
Step 7	**end** **Example:** `Device(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.

Verifying VRF Transfer for IP Sessions

Perform the following task as needed to verify VRF transfer for IP sessions. You can use the **show** commands in this task in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]]
4. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session uid** *session-identifier* **detail** **Example:** `Device# show subscriber session uid 4 detail`	Displays information about ISG subscriber sessions with a specific session identifier.
Step 3	**show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]] **Example:** `Device# show ip subscriber vrf vrf1`	Displays information about ISG IP subscriber sessions.
Step 4	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} **Example:** `Device# show idmgr session key nativeip-vrf ip-address 209.165.200.225`	Displays information related to ISG session and service identity.
Step 5	**show ip route** [**vrf** *vrf-name*] **Example:** `Device# show ip route`	Displays the current state of the routing table.

	Command or Action	Purpose
Step 6	**show ip dhcp binding** [**ip-address**] **Example:** `Device# show ip dhcp binding`	Displays address bindings on the Cisco IOS DHCP server.

Troubleshooting VRF Transfer for IP Sessions

The commands in this task can be used to troubleshoot VRF transfer of IP sessions. The **debug** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug subscriber** {**event** | **error** | **packet** | **policy** | **service**}
3. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
4. **debug subscriber policy dpm** {**error** | **event**}
5. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug subscriber** {**event**	**error**	**packet**	**policy**	**service**} **Example:** `Device# debug subscriber service`	Displays debugging messages pertaining to subscriber policies, policy server events, and changes to service.
Step 3	**debug ip subscriber** {**event**	**error**	**packet**	**fsm**	**all**} **Example:** `Device# debug ip subscriber error`	Displays debugging messages pertaining to an IP session created on the service gateway.
Step 4	**debug subscriber policy dpm** {**error**	**event**} **Example:** `Device# debug subscriber policy dpm event`	Displays diagnostic information about policy execution that is related to DHCP events.
Step 5	**debug ip dhcp server** {**events**	**packets**	**linkage**	**class**} **Example:** `Device# debug dhcp ip dhcp server events`	Enables Cisco IOS DHCP server debugging.

Configuration Examples for ISG Access for IP Subscriber Sessions

Example: Configuring ISG Routed IP Subscriber

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface 0/0/1.401 through a routed access network. ISG will create IP sessions upon receipt of DHCP DISCOVER packets, incoming valid IP packets, and RADIUS Access-Request packets.

```
interface GigabitEthernet 0/0/1.401
 ip subscriber routed
  initiator dhcp
  initiator unclassified ip-address
  initiator radius-proxy
```

Example: Creating ISG IP Interface Sessions

The following example shows how to configure an IP interface session on GigabitEthernet interface 0/0/1.401:

```
interface GigabitEthernet 0/0/1.401
 ip subscriber interface
```

Example: Creating ISG Static Sessions

The following example shows how to create an ISG static session for server 209.165.200.225 for subscribers who connect to ISG on GigabitEthernet interface 0/4 through a Layer 2-connected access network. ISG will create a static session upon receipt of valid source IP address.

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 0/4
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

Example: Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface0/0/1.401 through a Layer 2-connected access network. ISG will create IP sessions upon receipt of any frame with a valid source MAC address.

```
interface GigabitEthernet0/0/1.401
 ip subscriber l2-connected
  initiator unclassified mac-address
```

Example: Configuring IP Session Recovery for DHCP-Initiated IP Session

The following example shows how to configure an ISG policy that applies a service called “FIRST-SERVICE” upon session restart for subscribers belonging to the VRF “FIRST”:

```
class-map type control TEST
 match vrf FIRST
policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

Example: Configuring an ISG Interface for Dynamic DHCP Class Association

In the following example, GigabitEthernet interface 1/0/0.400 is configured with DHCP class-aware functionality, which enables ISG to influence DHCP IP address assignment. If the service SERVICE-DHCP is activated, the DHCP pool DHCP-POOL2 is used for address assignment. Otherwise, the default pool DHCP-POOL1 is used.

```
interface GigabitEthernet1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP-POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
ip dhcp class DHCP-CLASS2
!
policy-map type service SERVICE-DHCP
 classname DHCP-CLASS2
!
```

Example: Configuring DHCP Address Pool Classes and Relay Actions for ISG

This section contains examples of DHCP address pool configuration and relay actions for ISG.

DHCP Server Coresident with ISG Configuration

In the following configuration example, the ISPs are ISP1 and ISP2 companies. The ISP1 company has its addresses assigned from an address pool that is dynamically allocated using on-demand address pools (ODAP).

The ISP2 company has its customer addresses assigned from the address pool 10.100.0.0/16. Customers not associated with any ISP will have an address allocated from the address pool 10.1.0.0/16, and the lease time is set to 10 minutes.

```
!Address pool for ISP1 customers
ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool isp2-pool
 network 10.100.0.0 255.255.0.0
 class isp2
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

DHCP Relay Agent Coresident with ISG Configuration

In the following configuration example, there are two ISPs, “poolA” and “poolB”. The “poolA” ISP and its customers are allowed to have addresses in the ranges 10.1.0.0/16 and 10.3.0.0/16 and are relayed to the DHCP server at 10.55.10.1. The “poolB” ISP and its customers are allowed to have addresses in the range 10.2.0.0/16 and 10.4.0.0/16, and are relayed to the DHCP server at 10.10.2.1.

```
!Address ranges:
interface gigabitethernet1/0/0
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary
interface gigabitethernet2/0/0
 ip address 10.3.0.2 255.255.0.0
 ip address 10.4.0.2 255.255.0.0
!Address pools for poolA1 and poolB2:
 ip dhcp pool poolA1
 relay source 10.1.0.2 255.255.0.0
 class poolA1
 relay target 10.55.10.1
!Address pool for poolA2:
ip dhcp pool poolA2
 relay source 10.3.0.2 255.255.0.0
 class poolA2
 relay target 10.55.10.1
!Address pools for poolB1 and poolB2:
ip dhcp pool poolB1
 relay source 10.2.0.2 255.255.0.0
 class poolB1
 relay target 10.10.2.1
ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

Configuration of secure ARP for the relay uses the same configuration command as secure ARP uses on a DHCP server. It uses the **update arp** command in address-pool configuration mode. If the system allocates an address from this address pool, secure ARP is added to it. If the system relays a packet using this address pool, secure ARP is also added to it.

Example: Configuring ISG Dynamic VPN Selection

The following example shows a configuration in which subscribers are initially assigned an IP address from the DHCP global pool DHCP-POOL1. After a subscriber accesses the web portal and selects the Corporate VPN service, ISG performs a VRF transfer and the subscriber is assigned a new IP address from the DHCP pool, VPN-POOL1. In this case, a single multiservice interface is required.

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE-406a
 ip subscriber l2-connected
  initiator dhcp
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
 class default
!
ip dhcp class default
!
!
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN-POOL1
 vrf VPN-406-1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30
class DHCP-CLASS-VPN-406-1001
!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

Example: Troubleshooting DHCP Server User Authentication

You can determine the DHCP authentication by using the **debug ip dhcp server events**, **debug ip dhcp server packets**, and **debug subscriber policy dpm event** commands. The following is sample output from the **debug subscriber policy dpm event** command:

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address =
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address
001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the
SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

You can also use the **show subscriber session detailed** and **show ip dhcp binding** commands to display subscriber information and DHCP pool information. The following is sample output from the **show ip dhcp binding** command:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
DHCP configuration	*IP Addressing: DHCP Configuration Guide*
Configuring ISG control policies	"Configuring ISG Control Policies" module in the *Intelligent Services Gateway Configuration* Guide.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Access for IP Subscriber Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

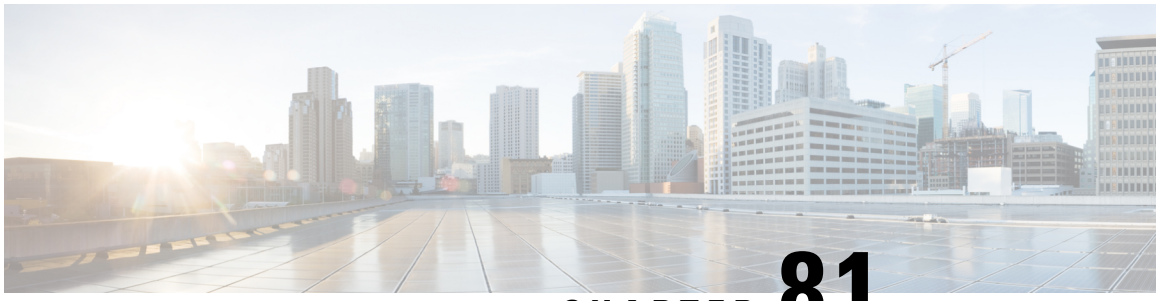
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 104: Feature Information for ISG Access for IP Subscriber Sessions

Feature Name	Releases	Feature Configuration Information
DHCP—Server User Authentication	Cisco IOS XE Release 3.1S	The DHCP Server User Authentication feature is used to authenticate the DHCP clients. The following commands were introduced or modified by this feature: **aaa authentication login** and **network** (DHCP).
IP Session Recovery for DHCP-Initiated IP Sessions	Cisco IOS XE Release 2.2	ISG provides a default policy and the ability to configure a policy that determines the actions ISG will take upon session restart following the recovery of a DHCP-initiated IP session. The following commands were introduced or modified by this feature: **class type control** and **match vrf**.
IP Subscriber Session CLI Updates	Cisco IOS XE Release 2.2	Some of the commands that are used to configure ISG IP subscriber sessions were modified or replaced. The following commands were introduced or modified by this feature: **clear ip subscriber**, **debug ip subscriber**, **identifier interface**, **identifier ip src-addr**, **initiator**, **interface multiservice**, **ip subscriber interface, ip subscriber**, and **show ip subscriber**.
ISG—Downstream Pass-Through and Idle Timer	Cisco IOS XE Release 3.6S	Enables IPv6 downstream traffic from an ISG interface to pass through to a subscriber without a subscriber session present. The following command was introduced by this feature: **passthru downstream ipv6**.

Feature Name	Releases	Feature Configuration Information
ISG Policy Control—DHCP Proxy	Cisco IOS XE Release 2.2	This feature enables ISG to dynamically interact with DHCP and apply policies that influence the IP addresses that DHCP assigns subscribers.
ISG Session Creation—Interface IP Session: L2	Cisco IOS XE Release 2.5.0	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.
ISG Session Creation—Interface IP Session: L3	Cisco IOS XE Release 2.5.0	ISG IP interface sessions include all IP traffic received on a specific physical or virtual interface. IP interface sessions are provisioned through the CLI; that is, a session is created when the IP interface session commands are entered.
ISG Session Creation—IP Session Protocol Event (DHCP)	Cisco IOS XE Release 2.2	Most ISG sessions are created upon detection of a data flow that cannot be affiliated with an already active session. ISG can be configured to create an IP session upon receipt of the first DHCP DISCOVER packet received from a subscriber.
ISG Session Creation—IP Session Subnet and Source IP: L2	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.
ISG Session Creation—IP Session Subnet and Source IP L3	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies across specific data flows. An IP subnet session is an ISG session that includes any IP traffic from a single IP subnet. A source-IP-based session includes traffic from a single source IP address.
ISG Session—Multicast Coexistence	Cisco IOS XE Release 2.5.0	The ISG Session Multicast Coexistence feature introduces the ability to host all the subscribers and services (data and multicast) on the same VLAN by enabling multicast and IP sessions to coexist on the same subinterface for Cisco ASR 10000 Series Aggregation Routers.
ISG Session—VRF Transfer	Cisco IOS XE Release 2.2	The ISG session is the primary component used for associating services and policies with specific data flows. ISG sessions are associated with virtual routing and forwarding instances when routing is required for the network service. ISG VRF transfer provides a means to dynamically switch an active session between virtual routing domains.
ISG—Static Session Creation	Cisco IOS XE Release 2.5.0	The ISG Static Session Creation feature enables administrator initiated static IP sessions. The following commands were introduced or modified by this feature: **initiator static subscriber list**, **ip source**, **ip subscriber list**, and **show ip subscriber list**.

Feature Name	Releases	Feature Configuration Information
L3 Routed Dual Stack	Cisco IOS XE Gibraltar 16.10.x	The L3 Routed Dual Stack feature allows both IPv4 and IPv6 L3 routed sessions to exist together as a part of the same session. To enables the functionality, you must configure the 'collect identifier mac-address' command at the beginning of the session.



CHAPTER 81

Configuring ISG IPv6 Support

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes the IPv6 support available for ISG IP subscriber sessions including information about the Time-Based Billing feature.

Restrictions for ISG IPv6 Support

- Out-of-band IPv6 sessions are not supported, which means DHCP initiated or RADIUS proxy initiated sessions are not supported for IPv6 sessions.
- Time-based billing is not supported on PPP sessions directly; it is supported through services and flows installed on the PPP session

Information About ISG IPv6 Support

ISG IPv6 Session Support

ISG creates an IPv6 subscriber session based on the first IPv6 packet received from an unclassified IPv6 address or IPv6 prefix, similar to the way subscriber sessions are created for IPv4 packets. The subscriber session is identified by the IPv6 address. Native IP sessions have either an IPv4 or IPv6 address, but not both. A native IPv6 session has an IPv6 address only and all traffic generated from the subscriber uses IPv6.

IPv6 single-stack sessions are supported for ISG subscriber sessions. If a native IP subscriber's host sends traffic for both an IPv4 and IPv6 address, ISG creates a separate IP session for each of these IP addresses. This subscriber will have an IPv4 session and an IPv6 session with no interaction between them. A dual-stack session is a single subscriber session with two distinct IP addresses, one for IPv4 and one for IPv6. Dual-stack native IP sessions are not supported.

Layer 3 unclassified IPv6 sessions for routed subscribers are supported. These sessions are identified by their unique IPv6 IP address or an IPv6 subnet session (IPv6 address and prefix). IPv6 is not supported for Layer 2 connected and DHCP-initiated subscriber sessions.

Session Coexistence on ISG Interfaces

The following session combinations can exist on the same ISG interface in Cisco IOS XE Release 3.5S and later releases:

- Native IPv6 and native IPv4 sessions
- Native IPv6 and PPP IPv4 sessions
- Native IPv6 and PPP IPv6 sessions
- Native IPv6 and PPP dual-stack sessions

ISG Dual-Stack Features

Dual-stack features are protocol independent and work at the session level. These features cannot be configured based on the stack. A single generic configuration is applied to the session regardless of whether it is a single-stack or dual-stack session. The configuration of these features is the same for IPv4 and IPv6.

Because these features are applied at the session level, the same instance of the feature handles both the IPv4 and IPv6 stacks for a dual-stack session, and the behavior is aggregated. For example, the same instance of the accounting feature counts both IPv4 and IPv6 packets. Similarly, the same instance of the idle timeout feature monitors both IPv4 and IPv6 traffic and considers a session to be idle when there is neither type of traffic.

The following features are examples of dual-stack features:

- Absolute Timeout (Session Timer)
- Idle Timeout (Connection Timer)
- ISG Accounting
- ISG Policer (Dynamic Rate Limiting)
- Quality of Service

ISG Protocol-Dependent Features

Protocol-dependent features rely on the underlying protocol. An instance of the feature works only for one of the protocols, either IPv6 or IPv4. For example, the Layer 4 Redirect feature has translation rules that are protocol dependent. An IPv6 packet can be redirected only to an IPv6 destination; an IPv4 packet can be redirected only to an IPv4 destination.

The configuration of protocol-dependent features applies only to the corresponding stack of the session. If a feature must run on both protocols for a dual-stack session, separate configurations must be created and applied on both stacks respectively. These features cannot be configured for an entire session unless it is a single-stack session.

The behavior of protocol-dependent features is limited to a single stack. An instance of the feature runs only on a particular stack and has no functional impact on the other stack, if applicable. If the feature is applied on

both stacks of a dual-stack session, two separate instances are created and run independently. There is no aggregated behavior for these features.

The following features are examples of ISG protocol-dependent features:

- Access Control Lists (ACLs)
- Layer 4 Redirect
- Port-Bundle Host Key
- Traffic Classes

IPv6 Support for ISG Features

The following ISG features are supported for native IPv6 sessions and PPP dual-stack sessions:

Feature	Description	Session Support
Absolute Timeout (Session Timer)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For configuration information, see the "Configuring ISG Policies for Session Maintenance" module in this guide.	• Native IPv4/IPv6 • PPP dual stack
Idle Timeout (Connection Timer)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For configuration information, see the "Configuring ISG Policies for Session Maintenance" module in this guide.	• Native IPv4/IPv6 • PPP dual stack
ISG Accounting	Per-session and per-service accounting can be configured on either an IPv4-only or IPv6-only IP session. Per-flow accounting can be configured on either an IPv4 or IPv6 traffic class. For configuration information, see the "Configuring ISG Accounting" module in this guide.	• Native IPv4/IPv6 • PPP dual stack
ISG Policer (Dynamic Rate Limiting)	IPv6 functionality and configuration are the same as for IPv4 subscriber sessions. For information, see the "Configuring MQC Support for IP Sessions" module in this guide.	• Native IPv4/IPv6 • PPP dual stack
Layer 4 Redirect	IPv6 packets can be redirected only to an IPv6 destination; IPv4 packets can be redirected only to an IPv4 destination. For configuration information, see the "Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module in this guide.	• Native IPv4/IPv6 • PPP dual stack • Protocol dependent

Feature	Description	Session Support
Modular QoS CLI (MQC)	The following operations are supported for an MQC policy applied to PPP IPv6 sessions and PPP dual-stack sessions: • Add or remove a class • Add, remove, or modify an action under a class • Modify an ACL For configuration information, see the "Configuring MQC Support for IP Sessions" module in this guide.	• Native IPv4 • PPP IPv6 • PPP dual stack
Traffic Classes	The protocol version of a traffic class is determined by the protocol version of the access control list (ACL) that was used to configure the traffic class. IPv6 traffic classes are supported using named IPv6 ACLs. Traffic classes are also supported on PPP sessions. For configuration information, see the "Configuring ISG Subscriber Services" module in this guide.	• Native IPv4/IPv6 • PPP dual stack • Protocol dependent

Time-Based Billing Service

The Time-Based Billing feature calculates the 24-hour volume usage for all subscriber sessions that are active on an L2TP network server (LNS) at a specified time each day. It reports the volume used by a session since the last specified time, in 24-hour intervals. You can configure the router to collect the volume statistics of all active sessions at the same time every day, for example, everyday at midnight. The system would report the volume usage of a session from midnight of the previous day to midnight of the current day.

Time-based billing will also report input and output traffic statistics for IPv6 and IPv4 traffic separately and as an aggregate using new AAA attributes in AAA accounting records.

Changes in local time based on Day Light Savings Time (DST), Network Time Protocol (NTP), or clock changes configured on the router are taken into account when reporting volume statistics at the specified time.

Time-based billing is supported for IPv4, IPv6, and PPP sessions.

How to Configure ISG IPv6 Support

For information on creating IPv6 subscriber sessions for routed ISG subscribers, see the module "Configuring ISG Access for IP Subscriber Sessions."

Note IPv6 sessions for Layer 2 connected subscribers are not supported.

Defining an IPv6 Prefix for ISG Subscriber Sessions

To enable ISG to create an IPv6 subscriber session after receiving the first packet with a particular IPv6 prefix, you define the IPv6 prefix in an IP subscriber list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ipv6 prefix default** *length*
5. **exit**
6. **interface** *type number*
7. **ip subscriber routed**
8. **initiator unclassified ip-address** [**ipv6**] [**list** *list-name*]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip subscriber list** *list-name* **Example:** `Router(config)# ip subscriber list mylist`	Specifies the IP subscriber list name and enters server list configuration mode.
Step 4	**ipv6 prefix default** *length* **Example:** `Router(config-server-list)# ipv6 prefix default 64`	Defines the IPv6 prefix for which ISG initiates IPv6 subscriber sessions.
Step 5	**exit** **Example:** `Router(config-server-list)# exit`	Returns to global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 2/0/0`	Specifies an interface and enters interface configuration mode.
Step 7	**ip subscriber routed** **Example:**	Specifies that routed IP subscribers are to be hosted on the interface and enters ISG IP subscriber configuration mode.

	Command or Action	Purpose
	`Router(config-if)# ip subscriber routed`	
Step 8	**initiator unclassified ip-address** [**ipv6**] [**list** *list-name*] **Example:** `Router(config-subscriber)# initiator unclassified ip-address ipv6 list mylist`	Enables ISG to create an IPv6 subscriber session after receiving a packet with the IPv6 prefix.
Step 9	**end** **Example:** `Router(config-subscriber)# end`	Returns to privileged EXEC mode.

Configuring Time-Based Billing Service

ISG time-based billing is configured in the service profile on a AAA server. If you include a traffic class in the service profile, time-based billing will apply to the specified flow. If you do not configure a traffic class, time-based billing will apply to the session.

Before you begin

ISG per-session or per-flow accounting must be configured.

SUMMARY STEPS

1. Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"
2. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
3. **show subscriber session feature time-based-billing detailed**

DETAILED STEPS

Step 1 Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"

Add the Post Paid VSA to the service profile. This attribute specifies the weekly tariff-billing points as follows:

hh:*mm*:*ss*:*d*—Weekly billing time.

- hh = hour of day <0–23>
- mm = minutes <0–59>
- ss = seconds <0–59>
- d = bitmap format for the days of week. Each weekday is represented by one bit, as follows:
  - 00000001 = Monday
  - 00000010 = Tuesday
  - 00000100 = Wednesday
  - 00001000 = Thursday
  - 00010000 = Friday
  - 00100000 = Saturday

• 01000000 = Sunday

Step 2 Cisco-AVpair = “ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]”

Add the ISG traffic class attribute to the service profile. This attribute specifies the input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

Step 3 **show subscriber session feature time-based-billing detailed**

Enter this command on the ISG router to display information about time-based billing. The following example shows output from this command:

```
Router# show subscriber session feature time-based-billing detailed

-------------------------------------------------
Type: IP, UID: 7, State: authen, Identity: aabb.cc00.6400
Session Up-time: 00:00:08, Last Changed: 00:00:08
Switch-ID: 4102

Time-based-billing:
Class-id   Dir  Last-Tariff  Packets-v4    Bytes-v4    Packets-v6 Bytes-v6  Source
0          In   1291415061   4             400         2          200       Peruser
1          Out  1291415061   3             200         1          100       Peruser
```

Configuration Examples for ISG IPv6 Support

Example: IPv6 Prefix for ISG Subscriber Sessions

The following example shows an IPv6 prefix defined in the IP subscriber list named mylist, which has been assigned to Gigabit Ethernet port 0/0/0. ISG will create an IPv6 subscriber session when it receives the first packet with the default IPv6 prefix.

```
ip subscriber list mylist
  ipv6 prefix default 64

interface GigabitEthernet0/0/0
 ip vrf forwarding vrf-1
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 out
 ip virtual-reassembly
 zone-member security private
 media-type sfp
 negotiation auto
 ipv6 address 2001:DB8:1:1::26/64
 ip subscriber routed
  initiator unclassified ip-address ipv6 list mylist
```

Example: Time-Based Billing Service

The following example shows an IPv6 session configured for doing billing daily at midnight:

```
PPW00:00:00:127
```

Day 1—A native IPv6 session starts at 10 a.m.

Day 1 at tariff-switch point (12 a.m.)—A snapshot of the current volume used from 10 a.m. is recorded, for example:

```
IPv6-input-bytes = 10000
IPv6-input-packets = 100
IPv6-output-bytes = 20000
IPv6-output-packets= 200
```

Day 2 say at 12:10 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 100          Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 10000         Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 100
Tariff-Input-Octets-IPv6 = 10000
Tariff-Output-Packets = 200         Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000        Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 200
Tariff-Output-Octets-IPv6 = 200
```

Day 2—All Interim records sent thereafter until the next tariff-switch point will carry the above values.

Day 2 at tariff-switch point (12 a.m.)—A snapshot of the volume used from Day 1 at 12 a.m. to Day 2 at 12 a.m. is recorded, for example:

```
IPv6-input-bytes = 600000
IPv6-input-packets = 6000
IPv6-output-bytes = 20000
IPv6-output-packets= 200
```

Day 3 say at 12:20 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 6000         Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 600000        Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 6000
Tariff-Input-Octets-IPv6 = 600000
Tariff-Output-Packets = 200         Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000        Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 200
Tariff-Output-Octets-IPv6 = 200
```

Day 3—All Interim records sent thereafter until the next tariff-switch point will carry the above same values.

Day 4—The session is disconnected at 8 a.m. A snapshot of the volume used from last tariff to the session disconnect time is taken, for example:

```
IPv6-input-bytes = 500
IPv6-input-packets = 1
IPv6-output-bytes = 400
IPv6-output-packets= 1
```

A stop record is sent with the following values in the VSAs:

```
Tariff-Input-Packets = 1            Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 500           Aggregate Input IPv4 and IPv6 Bytes
Tariff-Input-Packets-IPv6 = 1
```

```
Tariff-Input-Octets-IPv6 = 500
Tariff-Output-Packets = 1           Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 400          Aggregate Output IPv4 and IPv6 Bytes
Tariff-Output-Packets-IPv6 = 1
Tariff-Output-Octets-IPv6 = 400
```

The following example shows an IPv4 session configured for doing billing daily at midnight:

```
PPW00:00:00:127
```

Day 1—A native IPv4 session starts at 10 a.m.

Day 1 at tariff-switch point (12 a.m.)—A snapshot of the current volume used from 10 a.m. is recorded, for example:

```
IPv4-input-bytes = 10000
IPv4-input-packets = 100
IPv4-output-bytes = 20000
IPv4-output-packets= 200
```

Day 2 say at 12:10 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 100          Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 10000         Aggregate Input IPv4 and IPv6 Bytes
Tariff-Output-Packets = 200         Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000        Aggregate Output IPv4 and IPv6 Bytes
```

Day 2—All Interim records sent thereafter until the next tariff-switch point will carry the same above values.

Day 2 at tariff-switch point (12 a.m.)—A snapshot of the volume used from Day 1 at 12 a.m. to Day 2 at 12 a.m. is recorded, for example:

```
IPv4-input-bytes = 600000
IPv4-input-packets = 6000
IPv4-output-bytes = 20000
IPv4-output-packets= 200
```

Day 3 say at 12:20 a.m.—Interim record is sent. The Interim record will carry the following values in the VSAs:

```
Tariff-Input-Packets = 6000         Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 600000        Aggregate Input IPv4 and IPv6 Bytes
Tariff-Output-Packets = 200         Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 20000        Aggregate Output IPv4 and IPv6 Bytes
```

Day 3—All Interim records sent thereafter until the next tariff-switch point will carry the same above values.

Day 4—The session is disconnected at 8 a.m. A snapshot of the volume used from the last tariff-switch point to session disconnect time is taken, for example:

```
IPv4-input-bytes = 500
IPv4-input-packets = 1
IPv4-output-bytes = 400
IPv4-output-packets= 1
```

A stop record is sent with the following values in the VSAs:

```
Tariff-Input-Packets = 1            Aggregate Input IPv4 and IPv6 Packets
Tariff-Input-Octets = 500           Aggregate Input IPv4 and IPv6 Bytes
```

```
Tariff-Output-Packets = 1          Aggregate Output IPv4 and IPv6 Packets
Tariff-Output-Octets = 400         Aggregate Output IPv4 and IPv6 Bytes
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
IPv6 Configuration	IPv6 Configuration Guide, Cisco IOS XE Release 3S
Configuring ISG accounting	"Configuring ISG Accounting" module in this guide
Configuring ISG timers	"Configuring ISG Policies for Session Maintenance" module in this guide
Configuring Layer 4 redirect	"Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module in this guide
Configuring traffic classes	"Configuring ISG Subscriber Services" module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG IPv6 Support

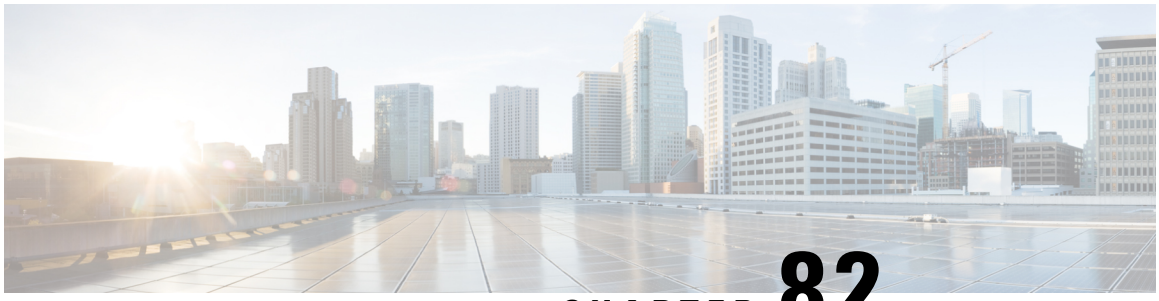
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 105: Feature Information for ISG IPv6 Support

Feature Name	Releases	Feature Information
ISG IPv6 Support	Cisco IOS XE Release 3.4S	Adds IPv6 support for routed IP subscriber sessions and for the following ISG features: • Absolute Timeout • Idle Timeout • ISG Accounting • Traffic Classes Adds the Time-Based Billing feature and traffic class support for services and flows on PPP sessions. **Note** Only single-stack sessions are supported for ISG subscriber sessions; dual-stack sessions are not supported. The following commands were introduced or modified: **initiator**, **ipv6 prefix**, **show ip subscriber**, **show subscriber session**.

Feature Name	Releases	Feature Information
ISG: IPv6 Support phase II	Cisco IOS XE Release 3.5S	Adds support for IPv6 PPP sessions and PPP dual-stack sessions for the following features: • HA-supported ISG features • ISG Policer • Layer 4 Redirect • MQC Adds support for PPP dual-stack sessions for the following features: • Absolute Timeout • Idle Timeout • ISG Accounting • Traffic Classes The following commands were introduced or modified: **redirect session-limit**, **redirect to**, **show redirect group**, **show redirect translations**, **server ip**.



CHAPTER 82

Configuring MQC Support for IP Sessions

The MQC Support for IP Sessions feature provides modular quality of service (QoS) command-line interface (CLI) provisioning on Cisco Intelligent Services Gateway (ISG) IP sessions. It makes the full set of modular QoS CLI (MQC) syntax available for the sessions, whether they are configured locally or downloaded from a remote authentication, authorization, and accounting (AAA) server.

Restrictions for MQC Support for IP Sessions

General Restrictions

- Creation of IP sessions over PPP sessions is not supported.

Note This document uses the generic term PPP to cover all protocol types. Examples of protocols include PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA).

- Only the marking and policing features work in upstream traffic. All queuing, policing, and marking MQC features work in downstream traffic.
- Class-level queues are allowed only at the child level in session policy maps. All other levels must have a single-level policy and use the default queues.
- Because IP sessions cannot be load-balanced, load balancing is not supported on any system.

Note Restrictions that are applicable to PPPoGEC with per-session QoS are also applicable to IPoGEC with per-session QoS. For more information, see PPPoGEC: Per Session QoS chapter of the *QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)*.

Information About MQC Support for IP Sessions

ISG Policers

You can create configurations to work on an IP session with multiple traffic classes, and with one or more of the traffic classes acting as a policer. ISG policer is retained for backward compatibility and is fully supported if you do not want to migrate to MQC now. Note that ISG policing is supported on traffic classes, but MQC is not supported for traffic classes.

An ISG session can be configured with the ISG policer (also called dynamic rate limiting) or MQC, but not both. You should either use the ISG policer or migrate fully to MQC. If you do not migrate fully from ISG policer to MQC, a misconfiguration will occur.

Precedence Order in Policy Maps

A policy map can be attached to one or more interfaces to specify a service policy. Configuration sources combined with context determines which QoS policy map is applied. The three configuration sources and their general order of precedence are as follows:

1. Per-user (per-subscriber) configuration
2. Service profile
3. Interface configuration

This order of precedence shows the general condition, that is, service profiles and per-user configurations have higher priority than interface configurations.

However, a change of authorization (CoA) per-user push replaces the current per-user configuration for any overlapping or common feature. Similarly, when a new service logs in, its configuration replaces any overlapping feature, from previously configured service profiles, that is not already in effect from a per-user configuration source

If the new service then logs off, the previously existing configuration is reapplied if no higher-precedence configuration source is in effect.

Given those precedence qualifications, the policy map is determined as follows:

- If there is no policy map on the session, the incoming policy map is not applied.
- If an existing policy map is configured from a higher priority source than an incoming one, the incoming policy map is not applied.
- If an existing policy map is configured from a lower priority source than an incoming one, the incoming policy map replaces it.

How to Configure MQC Support for IP Sessions

Configuring Local Subscriber Profile for MQC Support

To configure a QoS policy map to define a service policy, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **service-policy** *policy-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *service-name* **Example:** `Router# (config)# policy-map type service service1`	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.
Step 4	**service-policy** *policy-name* **Example:** `Router# (config-service-policymap)# service-policy service-policy1`	Configures the service policy.

What to do next

For information about configuring a local service profile, see the section “Configuring Per-Session QoS Using the ISG Framework” in the "Configuring ISG Control Policies" chapter in the *Intelligent Services Gateway Configuration Guide*.

Configuring ISG QoS for IP Sessions

To associate a previously configured traffic class with a policy map, perform these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-name*
4. **class type traffic** *class-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *service-name* **Example:** `Router# (config)# policy-map type service`	Enters policy-map configuration mode. Specifies the policy-map name and its service configuration.
Step 4	**class type traffic** *class-name* **Example:** `Router# (config-service-policymap)# class type traffic`	Associates a previously configured traffic class with the policy map.

Configuration Examples for MQC Support for IP Sessions

QoS Policy-Map Service Profile and Command Policy-Map Configurations Example

The following example shows how to configure a QoS policy map, a service profile, and a command policy map. The command policy map is then configured onto interface GigabitEthernet 0/0/0 with the **service-policy** keyword.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map match-any EF-customer
Router(config-cmap)# match access-group name CUSTOMER-EF
Router(config-cmap)# class-map match-any EF-WAN
Router(config-cmap)# match qos-group 6
Router(config-cmap)# policy-map PREMIUM_MARK_IN
```

```
Router(config-pmap)# class EF-customer
Router(config-pmap-c)# set cos 6
Router(config-pmap-c)# set dscp ef
Router(config-pmap-c)# set qos-group 6
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# set dscp af11
Router(config-pmap-c)# set qos-group 1
Router(config-pmap-c)# set cos 1
Router(config-pmap-c)# policy-map PREMIUM_UB_OUT
Router(config-pmap)# class EF-WAN
Router(config-pmap-c)# police cir 200000000
Router(config-pmap-c-police)# priority
Router(config-pmap-c)# class class-default
Router(config-pmap-c)# policy-map type service PREMIUM_SERVICE
Router(config-service-policymap)# service-policy input PREMIUM_MARK_IN
Router(config-service-policymap)# service-policy output PREMIUM_UB_OUT
Router(config-service-policymap)# policy-map type control INT
Router(config-control-policymap)# class type control always event account-logon
Router(config-control-policymap-class-control)# 1 service-policy type service name
PREMIUM_SERVICE
Router(config-control-policymap-class-control)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# pppoe enable group global
Router(config-if)# service-policy type control INT
```

Additional References

Related Documents

Related Topic	Document Title
How to configure ISG control policies	"Configuring ISG Control Policies module in this guide
How to configure QoS policies using the MQC	*Cisco IOS Quality of Service Solutions Configuration Guide*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

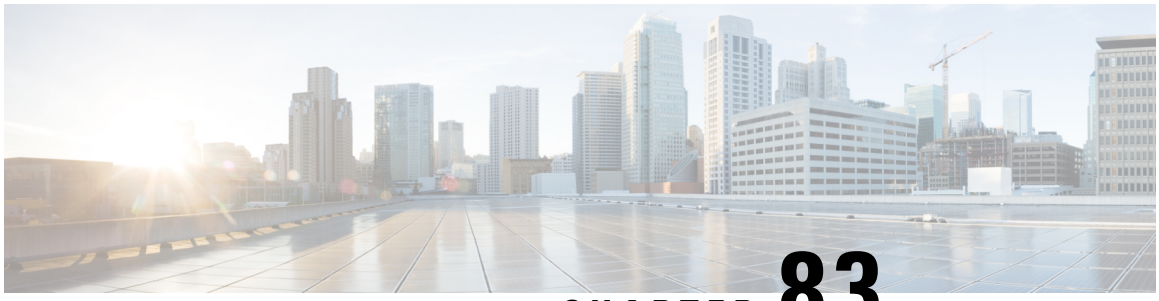
Feature Information for MQC Support for IP Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 106: Feature Information for MQC Support for IP Sessions

Feature Name	Releases	Feature Information
MQC Support for IP Sessions	Cisco IOS XE Release 2.2	Provides MQC provisioning on Cisco ISG IP sessions. The following commands were introduced or modified: **policy-map** and **service-policy**.



CHAPTER 83

Configuring ISG Port-Bundle Host Key

The Intelligent Services Gateway (ISG) provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure the ISG Port-Bundle Host Key feature, which maps TCP packets from subscribers to a local IP address for the ISG and a range of ports. This mapping allows an external portal to identify the ISG from which a session originated.

Prerequisites for the ISG Port-Bundle Host Key Feature

- The ISG Port-Bundle Host Key feature must be enabled separately at the portal and at all connected ISGs.
- All ISG source IP addresses configured with the **source** command must be routable in the management network where the portal resides.
- For each portal server, all connected ISGs must have the same port-bundle length.
- The external portal must support port-bundle host keys and must be configured with the same port-bundle host key parameters.

Restrictions for the ISG Port-Bundle Host Key Feature

- The ISG Port-Bundle Host Key feature uses TCP. Packets will not be mapped for a subscriber who does not send TCP traffic.
- Specifying the ISG Port-Bundle Host Key feature in a user profile works only when the user profile is available prior to the arrival of IP packets; for example, for PPP sessions or for DHCP-initiated IP sessions with transparent autologon.

Information About ISG Port-Bundle Host Key

Overview of ISG Port-Bundle Host Key

The ISG Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISG and a range of ports. This mapping allows the portal to identify the ISG from which the session originated. The mapping also identifies sessions uniquely even when subscribers have overlapping IP addresses. The ISG Port-Bundle Host Key feature enables a single portal to be deployed for multiple virtual routing and forwarding (VRF) instances even when there are subscribers with overlapping IP addresses.

Port-Bundle Host Key Mechanism

With the ISG Port-Bundle Host Key feature, an ISG performs Port-Address Translation (PAT) and Network Address Translation (NAT) on TCP traffic between the subscriber and the portal. When a subscriber TCP connection is set up, the ISG creates a port mapping that changes the source IP address to a configured ISG IP address and changes the source TCP port to a port allocated by the ISG. The ISG assigns a bundle of ports to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned port-bundle host key, or a combination of the port bundle and the ISG source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the portal server and the ISG in the Subscriber IP vendor-specific attribute (VSA). The table below describes the Subscriber IP VSA. When the portal server sends a reply to the subscriber, the ISG uses translation tables to identify the destination IP address and destination TCP port.

Table 107: Subscriber IP VSA Description

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Attribute Data
26	9	250 Account-Info	Subscriber IP	S *subscriber-ip-address* [:*port-bundle-number*] • S—Account-Info code for subscriber IP. • *subscriber-ip-address* [:*port-bundle-number*]—The port-bundle number is used only if the ISG Port-Bundle Host Key feature is configured.

For each TCP session between a subscriber and the portal, the ISG uses one port from the port bundle as the port map. Individual port mappings are flagged as eligible for reuse on the basis of inactivity timers, but are not explicitly removed once assigned. The number of port bundles is limited per ISG address, but there is no limit to the number of ISG IP addresses that can be configured for port bundle usage.

Note The ISG Port-Bundle Host Key feature assigns ISG IP addresses to the source IP in a round-robin fashion based on the available IP addresses and ports.

Port-Bundle Length

The port-bundle length is used to determine the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See the table below for available port-bundle length values and the resulting port-per-bundle and bundle-per-group values. You may want to increase the port-bundle length when you see frequent error messages about running out of ports in a port bundle.

Table 108: Port-Bundle Lengths and Resulting Port-per-Bundle and Bundle-per-Group Values

Port-Bundle Length (in Bits)	Number of Ports per Bundle	Number of Bundles per Group (and per ISG Source IP Address)
0	1	64512
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

Note For each portal server, all connected ISGs must have the same port-bundle length, which must correspond to the configured value given in the portal server's BUNDLE_LENGTH argument. If you change the port-bundle length on an ISG, be sure to make the corresponding change in the configuration on the portal.

Benefits of ISG Port-Bundle Host Key

Support for Overlapped Subscriber IP Addresses Extended to Include External Portal Usage

The ISG Port-Bundle Host Key feature enables external portal access regardless of the subscriber IP address or VRF membership. Without the use of port-bundle host keys, all subscribers accessing a single external portal must have unique IP addresses. Furthermore, because port-bundle host keys isolate VRF-specific addresses from the domain in which the portal resides, routing considerations are simplified.

Portal Provisioning for Subscriber and ISG IP Addresses No Longer Required

Without the ISG Port-Bundle Host Key feature, a portal must be provisioned for subscriber and ISG IP addresses before the portal is able to send RADIUS packets to the ISG or HTTP packets to subscribers. The ISG Port-Bundle Host Key feature eliminates the need to provision a portal to allow one portal server to serve multiple ISGs and one ISG to be served by multiple portal servers.

How to Configure ISG Port-Bundle Host Key

Enabling the ISG Port-Bundle Host Key Feature in a Service Policy Map

Perform this task to enable the ISG Port-Bundle Host Key feature in a service policy map. The ISG Port-Bundle Host Key feature will be applied to any subscriber who uses this service policy map.

Note We recommend that you use a dedicated service policy for the feature. Do not share a policy with other ISG features.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **ip portbundle**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** `Router(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an ISG service.

	Command or Action	Purpose
Step 4	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key feature for the service.
Step 5	**end** **Example:** `Router(config-service-policymap)# end`	(Optional) Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method for activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Enabling the ISG Port-Bundle Host Key Feature in a User Profile or Service Profile on the AAA Server

SUMMARY STEPS

1. Add the Port-Bundle Host Key attribute to the user or service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Port-Bundle Host Key attribute to the user or service profile. **Example:** `26,9,1 = "ip:portbundle=enable"`	Enables the ISG Port-Bundle Host Key feature in the user or service profile.

What to Do Next

If you enabled the ISG Port-Bundle Host Key feature in a service profile, you may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Configuring Port-Bundle Host Key Parameters

Perform this task to configure ISG Port-Bundle Host Key parameters and specify the interface for which ISG will use translation tables to derive the IP address and port number for downstream traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip portbundle**
4. **match access-list** *access-list-number*
5. **length** *bits*
6. **source** *interface-type interface-number*
7. **exit**
8. **interface** *type number*
9. **ip portbundle outside**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip portbundle** **Example:** `Router(config)# ip portbundle`	Enters IP portbundle configuration mode.
Step 4	**match access-list** *access-list-number* **Example:** `Router(config-portbundle)# match access-list 101`	Specifies packets for port mapping by specifying an access list to compare against the subscriber traffic.
Step 5	**length** *bits* **Example:** `Router(config-portbundle)# length 5`	Specifies the ISG port-bundle length, which determines the number of ports per bundle and bundles per group. • The default number of bits is 4. • See the section “Port-Bundle Length” for more information.
Step 6	**source** *interface-type interface-number* **Example:** `Router(config-portbundle)# source loopback 0`	Specifies the interface for which the main IP address is mapped by ISG to the destination IP addresses in subscriber traffic. • We recommend that you use a loopback interface as the source interface.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-portbundle)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/0`	Specifies an interface for configuration and enters the interface configuration mode.
Step 9	**ip portbundle outside** **Example:** `Router(config-if)# ip portbundle outside`	Configures ISG to reverse translate the destination IP address and TCP port to the actual subscriber IP address and TCP port for traffic going from the portal to the subscriber for the interface being configured.
Step 10	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Verifying the ISG Port-Bundle Host Key Configuration

SUMMARY STEPS

1. **enable**
2. **show ip portbundle status** [**free** | **inuse**]
3. **show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number*
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip portbundle status** [**free**	**inuse**] **Example:** `Router# show ip portbundle status free`	Displays information about ISG port-bundle groups.
Step 3	**show ip portbundle ip** *portbundle-ip-address* **bundle** *port-bundle-number* **Example:**	Displays information about a specific ISG port bundle.

	Command or Action	Purpose
	`Router# show ip portbundle ip 10.10.10.10 bundle 65`	
Step 4	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Configuration Examples for ISG Port-Bundle Host Key

Example: Configuring ISG Port-Bundle Host Key

The following example shows how to apply the ISG Port-Bundle Host Key feature to all sessions:

```
policy-map type service ISGPBHKService
 ip portbundle
!
policy-map type control PBHKRule
 class type control always event session-start
  1 service-policy type service ISGPBHKService
!
service-policy type control PBHKRule
interface gigabitethernet0/0/0
 ip address 10.1.1.1 255.255.255.0
 ip portbundle outside
!
ip portbundle
 match access-list 101
 length 5
 source loopback 0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

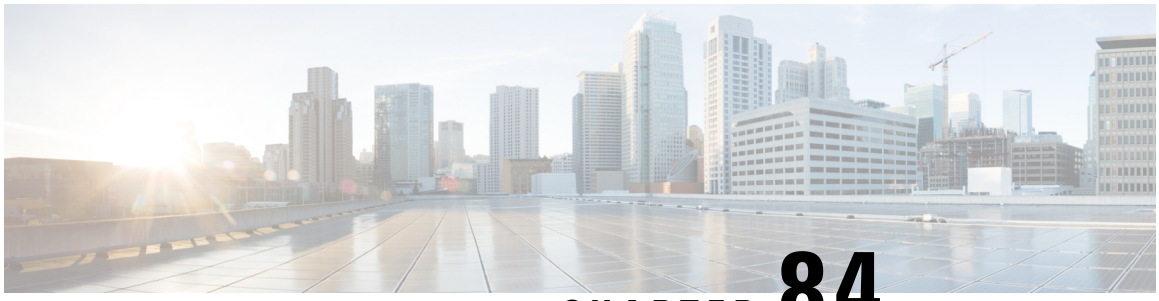
Feature Information for ISG Port-Bundle Host Key

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 109: Feature Information for ISG Port-Bundle Host Key

Feature Name	Releases	Feature Configuration Information
ISG Port-Bundle Host Key	Cisco IOS XE Release 2.2	The ISG Port-Bundle Host Key feature serves as an in-band signaling mechanism for session identification at external portals. TCP packets from subscribers are mapped to a local IP address for the ISG and a range of ports. This mapping allows the portal to identify the ISG from which the session originated.



CHAPTER 84

Configuring ISG as a RADIUS Proxy

Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. The ISG RADIUS proxy feature enables ISG to serve as a proxy between a client device that uses RADIUS authentication and an authentication, authorization, and accounting (AAA) server. When configured as a RADIUS proxy, ISG is able to "sniff" (look at) the RADIUS packet flows and, on successful authentication, it can transparently create a corresponding ISG session. This module describes how to configure ISG as a RADIUS proxy.

In public wireless LAN (PWLAN) deployments, service providers must absolutely ensure the billing accuracy of a user's session. The billing accuracy must also be met in case of a network component failure. The RADIUS proxy billing accuracy feature ensures that the start and stop session events are accurate and the events are the main references for session management.

Prerequisites for ISG RADIUS Proxy

The Cisco software image must support authentication, accountability and authorization (AAA) and Intelligent Services Gateway (ISG).

Restrictions for ISG RADIUS Proxy

Wireless Internet service provider roaming (WISPr) attributes are not supported.

Information About ISG RADIUS Proxy

Overview of ISG RADIUS Proxy

Public wireless LANs (PWLANs) and wireless mesh networks can contain hundreds of access points, each of which must send RADIUS authentication requests to an authentication, addressing and authorization (AAA) server. The Intelligent Services Gateway (ISG) RADIUS proxy functionality allows the access points to send authentication requests to ISG, rather than directly to the AAA server. ISG relays the requests to the AAA server. The AAA server sends a response to ISG, which then relays the response to the appropriate access point.

When serving as a RADIUS proxy, ISG can pull user-specific data from the RADIUS flows that occur during subscriber authentication and authorization, and transparently create a corresponding IP session upon successful authentication. This functionality provides an automatic login facility with respect to ISG for subscribers that are authenticated by devices that are closer to the network edge.

When configured as a RADIUS proxy, ISG proxies all RADIUS requests generated by a client device and all RADIUS responses generated by the corresponding AAA server, as described in RFC 2865, RFC 2866, and RFC 2869.

ISG RADIUS proxy functionality is independent of the type of client device and supports standard authentication (that is, a single Access-Request/Response exchange) using both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), Access-Challenge packets, and Extensible Authentication Protocol (EAP) mechanisms.

In cases where authentication and accounting requests originate from separate RADIUS client devices, ISG associates all requests with the appropriate session through the use of correlation rules. For example, in a centralized PWLAN deployment, authentication requests originate from the wireless LAN (WLAN) access point, and accounting requests are generated by the Access Zone Router (AZR). The association of the disparate RADIUS flows with the underlying session is performed automatically when the Calling-Station-ID (Attribute 31) is sufficient to make the association reliable.

Following a successful authentication, authorization data collected from the RADIUS response is applied to the corresponding ISG session.

Sessions that were created using ISG RADIUS proxy operation are generally terminated by receipt of an Accounting-Stop packet.

To configure RADIUS proxy billing, you can use the **timer reconnect** command and **show radius-proxy session** command in the appropriate configuration modes.

To enable session reconnection for ISG RADIUS proxy servers and clients, use **pwlan-session reconnect** command in the appropriate configuration mode.

ISG RADIUS Proxy Handling of Accounting Packets

By default, ISG RADIUS proxy responds locally to accounting packets it receives. The **accounting method-list** command can be used to configure ISG to forward RADIUS proxy client accounting packets to a specified server. Forwarding of accounting packets can be configured globally for all RADIUS proxy clients or on a per-client basis.

RADIUS Client Subnet Definition

If Intelligent Services Gateway (ISG) is acting as a proxy for more than one client device, all of which reside on the same subnet, the clients may be configured using a subnet definition rather than a discrete IP address for each device. This configuration method results in the sharing of a single configuration by all the client devices.

ISG RADIUS Proxy Support for Mobile Wireless Environments

ISG RADIUS proxy uses mobile wireless-specific processes to provide support for Gateway General Packet Radio Service (GPRS) Support Node (GGSN) environments.

Attribute Processing and RADIUS Request Correlation

When authentication and accounting requests originate from separate RADIUS client devices, ISG uses correlation rules to associate all the requests with the appropriate session. The association of the disparate RADIUS flows with the underlying session is performed automatically when the Calling-Station-ID (Attribute 31) is sufficient to make the association reliable.

In mobile wireless environments, attribute processing and the correlation of RADIUS requests with a session are implemented differently than in a PWLAN environment. For example, in a PWLAN environment the Attribute 31 is a MAC address, and in a GGSN environment Attribute 31 is a Mobile Station Integrated Services Digital Network (MSISDN), which is a plain number or alphanumeric string. In addition, in a GGSN environment the correlation of RADIUS requests can be performed using attributes other than Attribute 31.

ISG RADIUS proxy supports mobile wireless environments by allowing you to specify whether the RADIUS-proxy client uses a MAC or MSISDN format for Attribute 31. The format is specified using the **calling-station-id format** command. In addition, you can use the **session-identifier** command to configure ISG RADIUS proxy to use other attributes (apart from Attribute 31) to perform RADIUS request correlation.

3GPP Attribute Support

In GGSN environments, ISG RADIUS proxy must understand and parse the Third Generation Partnership Project (3GPP) attributes described in the table below. These attributes form part of the accounting requests.

Table 110: 3GPP Attributes Supported by ISG RADIUS Proxy

Attribute	Description	Vendor ID/type
3GPP-IMSI	International Mobile Subscriber Identity (IMSI) for the user.	10415/1
3GPP-Charging-ID	Charging ID for this Packet Data Protocol (PDP) context (this together with the GGSN address constitutes a unique identifier for PDP context).	10415/2
3GPP-SGSN-Address	Serving GPRS Support Node (SGSN) address that is used by the GPRS Tunneling Protocol (GTP) control plane for handling of control messages. It may be used to identify the Public Line Mobile Network (PLMN) to which the user is attached.	10415/6

Benefits of ISG RADIUS Proxy

Use of Intelligent Services Gateway (ISG) RADIUS proxy has the following benefits:

- Allows the complete set of ISG functionality to be applied to extensible authentication protocol (EAP) subscriber sessions.
- Allows an ISG device to be introduced into a network with minimum disruption to the existing network access server (NAS) and authentication, authorization and accounting (AAA) servers.
- Simplifies RADIUS server configuration because only the ISG, not every access point, must be configured as a client.

How to Configure ISG as a RADIUS Proxy

Initiating ISG RADIUS Proxy IP Sessions

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/subslot/port*
4. **ip subscriber** {**interface** | **l2-connected** | **routed**}
5. **initiator radius-proxy**
6. **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** *type slot/subslot/port* **Example:** `Device(config)# interface GigabitEthernet 2/1/0`	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip subscriber** {**interface**	**l2-connected**	**routed**} **Example:**	Enables Intelligent Services Gateway (ISG) IP subscriber support on an interface, specifies the access method used

	Command or Action	Purpose
	`Device(config-if)# ip subscriber routed`	by IP subscribers to connect to ISG on an interface, and enters subscriber configuration mode.
Step 5	**initiator radius-proxy** **Example:** `Device(config-subscriber)# initiator radius-proxy`	Configures ISG to initiate IP sessions upon receipt of any RADIUS packet.
Step 6	**end** **Example:** `Device(config-subscriber)# end`	Exits the subscriber configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Global Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **pwlan-session reconnect**
6. **session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*}
7. **calling-station-id format** {**mac-address** | **msisdn**}
8. **accounting method-list** {*method-list-name* | **default**}
9. **accounting port** *port-number*
10. **authentication port** *port-number*
11. **key** [**0** | **7**] *word*
12. **timer** {**ip-address** | **request**} *seconds*
13. **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.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization and accounting (AAA) access control model.
Step 4	**aaa server radius proxy** **Example:** `Device(config)# aaa server radius proxy`	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	**pwlan-session reconnect** **Example:** `Device(config-locsvr-proxy-radius)# pwlan-session reconnect`	Enables the Public Wireless LAN (PWLAN) session reconnect feature.
Step 6	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*} **Example:** `Device(config-locsvr-proxy-radius)# session-identifier attribute 1`	(Optional) Correlates the RADIUS server requests of a session and identifies the session in the RADIUS proxy module.
Step 7	**calling-station-id format** {**mac-address** | **msisdn**} **Example:** `Device(config-locsvr-proxy-radius)# Calling-Station-ID format msisdn`	Specifies the Calling-Station-ID format.
Step 8	**accounting method-list** {*method-list-name* | **default**} **Example:** `Device(config-locsvr-proxy-radius)# accounting method-list fwdacct`	Specifies the server to which accounting packets from RADIUS clients are forwarded. **Note** By default, ISG RADIUS proxy handles accounting packets locally.
Step 9	**accounting port** *port-number* **Example:** `Device(config-locsvr-proxy-radius)# accounting port 2222`	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. • The default port is 1646.
Step 10	**authentication port** *port-number* **Example:** `Device(config-locsvr-proxy-radius)# authentication port 1111`	Specifies the port for which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.

	Command or Action	Purpose
Step 11	**key** [**0** | **7**] *word* **Example:** `Device(config-locsvr-proxy-radius)# key radpro`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 12	**timer** {**ip-address** | **request**} *seconds* **Example:** `Device(config-locsvr-proxy-radius)# timer ip-address 5`	Specifies the amount of time for which ISG waits for the specified event before terminating the session.
Step 13	**end** **Example:** `Device(config-locsvr-proxy-radius)# end`	Exits the ISG RADIUS proxy server configuration mode and returns to privileged EXEC mode.

Configuring ISG RADIUS Proxy Client-Specific Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **client** {**name** \| *ip-address*} [*subnet-mask* [**vrf** *vrf-id*]]
6. **pwlan-session reconnect**
7. **session-identifier** {**attribute** *number* \| **vsa vendor** *id* **type** *number*}
8. **calling-station-id format** {**mac-address** \| **msisdn**}
9. **accounting method-list** {*method-list-name* \| **default**}
10. **accounting port** *port-number*
11. **authentication port** *port-number*
12. **key** [**0** \| **7**] *word*
13. **timer** {**ip-address** \| **reconnect** \| **request**} *seconds*
14. **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	**aaa new-model** **Example:** `Device(config)# new-model`	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	**aaa server radius proxy** **Example:** `Device(config)# aaa server radius proxy`	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	**client** {**name** | *ip-address*} [*subnet-mask* [**vrf** *vrf-id*]] **Example:** `Device(config-locsvr-proxy-radius)# client 172.16.54.45 vrf myvrftable`	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS client configuration mode.
Step 6	**pwlan-session reconnect** **Example:** `Device(config-locsvr-radius-client)# pwlan-session reconnect`	Enables the Public Wireless LAN (PWLAN) session reconnect feature.
Step 7	**session-identifier** {**attribute** *number* | **vsa vendor** *id* **type** *number*} **Example:** `Device(config-locsvr-radius-client)# session-identifier vsa vendor 5335 type 123`	(Optional) Correlates the RADIUS requests of a session and identifies the session in the RADIUS proxy module.
Step 8	**calling-station-id format** {**mac-address** | **msisdn**} **Example:** `Device(config-locsvr-radius-client)# calling-station-id format msisdn`	Specifies the Calling-Station-ID format.
Step 9	**accounting method-list** {*method-list-name* | **default**} **Example:** `Device(config-locsvr-radius-client)# accounting method-list fwdacct`	Specifies the server to which accounting packets from RADIUS clients are forwarded.
Step 10	**accounting port** *port-number* **Example:**	Specifies the port on which the ISG listens for accounting packets from RADIUS clients.

	Command or Action	Purpose
	`Device(config-locsvr-radius-client)# accounting port 2222`	• The default port is 1646.
Step 11	**authentication port** *port-number* **Example:** `Device(config-locsvr-radius-client)# authentication port 1111`	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.
Step 12	**key** [**0** | **7**] *word* **Example:** `Device(config-locsvr-radius-client)# key radpro`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 13	**timer** {**ip-address** | **reconnect** | **request**} *seconds* **Example:** `Device(config-locsvr-radius-client)# timer ip-address 5`	Specifies the amount of time ISG waits for the specified event before terminating the session.
Step 14	**end** **Example:** `Device(config-locsvr-radius-client)# end`	Exits the ISG RADIUS client configuration mode and returns to privileged EXEC mode.

Defining an ISG Policy for RADIUS Proxy Events

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization radius-proxy** {**default** | *list-name*} *method1* [*method2* [*method3...*]]
5. **policy-map type control** *policy-map-name*
6. **class type control** {*control-class-name* | **always**} **event session-start**
7. *action-number* **proxy** [**aaa list** {**default** | *list-name*}]
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa authorization radius-proxy** {**default** | *list-name*} *method1* [*method2* [*method3...*]] **Example:** `Device(config)# aaa authorization radius-proxy RP group radius`	Configures AAA authorization methods for ISG RADIUS proxy subscribers.
Step 5	**policy-map type control** *policy-map-name* **Example:** `Device(config)# policy-map type control proxyrule`	Creates or modifies a control policy map, which defines an ISG control policy and enters control policy-map configuration mode.
Step 6	**class type control** {*control-class-name* | **always**} **event session-start** **Example:** `Device(config-control-policymap-class-control)# class type control always event session-start`	Specifies a control class for which actions may be configured and enters control policy-map class configuration mode.
Step 7	*action-number* **proxy** [**aaa list** {**default** | *list-name*}] **Example:** `Device(config-control-policymap-class-control)# 1 proxy aaa list RP`	Sends RADIUS packets to the specified server. • Use this command to configure ISG to forward RADIUS proxy packets to the server specified by the **aaa authorization radius-proxy** command in Step 4.
Step 8	**end** **Example:** `Device(config-control-policymap-class-control)# end`	Exits the config-control policymap-class-control mode and returns to privileged EXEC mode.

Verifying ISG RADIUS Proxy Configuration

SUMMARY STEPS

1. **show radius-proxy client** *ip-address* [**vrf** *vrf-id*]
2. **show radius-proxy session** {**id** *id-number* | **ip** *ip-address*}
3. **show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier* | **username** *username*] [**detailed**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show radius-proxy client** *ip-address* [**vrf** *vrf-id*] **Example:** `Device# show radius-proxy client 10.10.10.10`	Displays RADIUS proxy configuration information and a summary of sessions for an ISG RADIUS proxy client.
Step 2	**show radius-proxy session** {**id** *id-number* | **ip** *ip-address*} **Example:** `Device# show radius-proxy session ip 10.10.10.10`	Displays information about an ISG RADIUS proxy session. **Note** The ID can be found in the output of the **show radius-proxy client** command.
Step 3	**show subscriber session** [**identifier** {**authen-status** {**authenticated** | **unauthenticated**} | **authenticated-domain** *domain-name* | **authenticated-username** *username* | **dnis** *dnis* | **media** *type* | **nas-port** *identifier* | **protocol** *type* | **source-ip-address** *ip-address subnet-mask* | **timer** *timer-name* | **tunnel-name** *name* | **unauthenticated-domain** *domain-name* | **unauthenticated-username** *username*} | **uid** *session-identifier* | **username** *username*] [**detailed**] **Example:** `Device# show subscriber session detailed`	Displays information about subscriber sessions on an ISG device.

Clearing ISG RADIUS Proxy Sessions

SUMMARY STEPS

1. **enable**
2. **clear radius-proxy client** *ip-address*
3. **clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear radius-proxy client** *ip-address* **Example:** `Device# clear radius-proxy client 10.10.10.10`	Clears all ISG RADIUS proxy sessions that are associated with the specified client device.
Step 3	**clear radius-proxy session** {**id** *id-number* | **ip** *ip-address*} **Example:** `Device# clear radius-proxy session ip 10.10.10.10`	Clears a specific ISG RADIUS proxy session. **Note** The ID can be found in the output of the **show radius-proxy client** command.

Examples for Configuring ISG as a RADIUS Proxy

ISG RADIUS Proxy Configuration Example

The following example configures ISG to serve as a RADIUS proxy and to send RADIUS packets to the method list called RP. FastEthernet interface 0/0 is configured to initiate IP sessions upon receipt of RADIUS packets.

```
!
aaa new-model
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
aaa authorization radius-proxy RP group EAP
aaa accounting network FWDACCT start-stop group EAP
aaa accounting network FLOWACCT start-stop group EAP
!
aaa server radius proxy
session-identifier attribute 1
calling-station-id format msisdn
authentication port 1111
accounting port 2222
key radpro
message-authenticator ignore
! The method list "FWDACCT" was configured by the aaa accounting network FWDACCT
! start-stop group EAP command above.
accounting method-list FWDACCT
client 10.45.45.2
timer request 5
!
client 10.45.45.3
key aashica#@!$%&/
```

```
timer ip-address 120
!
!
! This control policy references the method list called "RP" that was configured using the
 aaa authorization radius-proxy command above.
policy-map type control PROXYRULE
class type control always event session-start
1 proxy aaa list RP
!
!
!
bba-group pppoe global
!
!
interface GigabitEthernet 2/1/0
ip address 10.45.45.1 255.255.255.0
ip subscriber routed
initiator radius-proxy
no ip route-cache cef
no ip route-cache
no cdp enable
!
! The control policy "PROXYRULE" is applied to the interface.
service-policy type control PROXYRULE
!
!
radius-server host 10.2.36.253 auth-port 1812 acct-port 1813 key cisco
radius-server host 10.76.86.83 auth-port 1665 acct-port 1666 key rad123
radius-server vsa send accounting
radius-server vsa send authentication
aaa new-model
!
!
aaa group server radius EAP
server 10.2.36.253 auth-port 1812 acct-port 1813
!
```

Example: ISG RADIUS Proxy and Layer 4 Redirect

```
aaa authorization network default local
!
redirect server-group REDIRECT
 server ip 10.255.255.28 port 23
 !
class-map type traffic match-any traffic1
match access-group input 101
!
policy-map type service service1
 class type traffic traffic1
  redirect list 101 to group REDIRECT
!
policy-map type control PROXYRULE
 class type control always event session-start
  1 proxy aaa list RP
  2 service-policy type service name service1
!
access-list 101 permit tcp host 10.45.45.2 any
```

The following is sample output from the containing RADIUS proxy details using the **show subscriber session** command, which displays RADIUS proxy details:

```
Device# show subscriber session username 12345675@example

Unique Session ID: 66
Identifier: aash
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:40, Last Changed: 00:00:00
Policy information:
  Authentication status: authen
  Active services associated with session:
    name "service1", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map PROXYRULE
      condition always event session-start
        1 proxy aaa list RP
        2 service-policy type service name service1
Session inbound features:
Feature: Layer 4 Redirect
Traffic classes:
  Traffic class session ID: 67
   ACL Name: 101, Packets = 0, Bytes = 0
Unmatched Packets (dropped) = 0, Re-classified packets (redirected) = 0
Configuration sources associated with this session:
Service: service1, Active Time = 00:00:40
Interface: FastEthernet0/1, Active Time = 00:00:40
```

Additional References for Configuring ISG as a RADIUS Proxy

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Overview of ISG RADIUS proxy	*Configuring Intelligent Service Gateway Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2869	RADIUS Extensions

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring ISG as a RADIUS Proxy

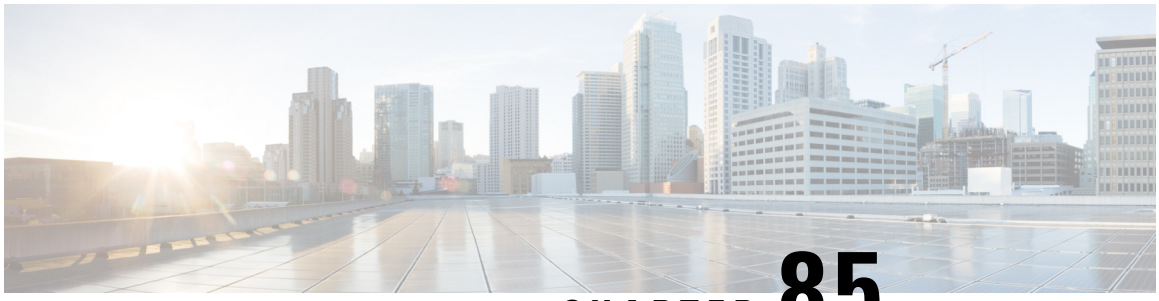
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 111: Feature Information for Configuring ISG as a RADIUS Proxy

Feature Name	Releases	Feature Information
RADIUS Proxy Enhancements for ISG	Cisco IOS XE Release 2.2	RADIUS proxy enhancements enable ISG to serve as a proxy between a client device that uses RADIUS authentication and an AAA server. This functionality enables ISG to be deployed in PWLAN and wireless mesh networks where authentication requests for mobile subscribers must be sent to specific RADIUS servers. The following commands were introduced or modified by this feature: **aaa authorization radius-proxy**, **aaa server radius proxy**, **accounting method-list**, **accounting port**, **authentication port**, **clear radius-proxy client**, **clear radius-proxy session**, **client (ISG RADIUS proxy)**, **debug radius-proxy**, **initiator radius-proxy**, **key (ISG RADIUS proxy)**, **message-authenticator ignore**, **proxy (ISG RADIUS proxy)**, **show radius-proxy client**, **show radius-proxy session**, **timer (ISG RADIUS proxy)**.
ISG—AAA Wireless Enhancements	Cisco IOS XE Release 2.5.0	AAA Wireless Enhancements enable ISG RADIUS proxy to provide additional support for mobile wireless environments. It includes changes to RADIUS attribute 31 processing. The following commands were introduced by this feature: **session-identifier**, **calling-station-id format**.

Feature Name	Releases	Feature Information
ISG—Authentication:RADIUS Proxy WiMax Enhancements	Cisco IOS XE Release 2.5.0	This feature enhances ISG RADIUS proxy to provide additional support for WiMax broadband environments.
ISG—PWLAN Reconnect	Cisco IOS XE Release 3.8S	PWLAN Reconnect enhances user authentication and security while authenticating over PWLAN networks. The following command was introduced by this feature: **pwlan-session reconnect**.



CHAPTER 85

Configuring ISG as a RADIUS Proxy in Passthrough Mode

Configuring ISG as a RADIUS Proxy in Passthrough Mode allows the Cisco Intelligent Services Gateway (ISG) acting as a RADIUS Proxy to direct all the RADIUS traffic from the client to the RADIUS server, without creating an ISG session.

This module describes how to configure ISG in RADIUS Proxy passthrough mode.

Prerequisites for Configuring ISG as a RADIUS Proxy in Passthrough Mode

- You need to configure the authentication and accounting methods.
- You need to configure the AAA server.

Restrictions for Configuring ISG as a RADIUS Proxy in Passthrough Mode

- High availability for RADIUS proxy passthrough is not supported. However, once, the switchover is completed, new sessions are entertained.

Information About Configuring ISG as a RADIUS Proxy in Passthrough Mode

ISG Acting as a RADIUS Proxy Passthrough

The RADIUS proxy module of the Cisco ISG can be run in the passthrough mode to proxy the client's RADIUS traffic. This improves manageability. The RADIUS Proxy passthrough mode can be configured in two ways:

- Global level: You can enable RADIUS proxy passthrough globally by configuring the **mode pass-through** command in the ISG RADIUS proxy server configuration mode. This causes all the clients configured after this command to be in RADIUS Proxy passthrough mode.
- Client level: You can enable RADIUS proxy passthrough at the client level by configuring the **mode pass-through** command for a specific client in the RADIUS proxy client configuration mode.

Note The ISG interface can also be configured for dual initiators where one initiator can be RADIUS proxy and the other non-RADIUS proxy. When a specified ISG interface having dual initiators receives the non-RADIUS proxy trigger, ISG creates a session for the client. However, if this interface has a client configured to be in RADIUS proxy pass-through mode, it does not create a session when the RADIUS proxy trigger is received. Both these scenarios can co-exist on the same ISG interface.

The RADIUS proxy configuration allows you to configure the accounting method list which specifies the AAA server to which the accounting start, interim and stop records are forwarded. This can be done at both the client level and the global level.

Benefits of Using ISG in RADIUS Proxy Passthrough Mode

- RADIUS proxy passthrough mode offers more security as the AAA server's IP address is hidden from the ultimate host.
- Performance is improved as ISG sessions are not created for RADIUS clients.
- The same ISG can serve in two different modes as listed below:
  - ISG acting as a RADIUS proxy where a session is created and the client's RADIUS messages are sent to an external AAA server.
  - ISG acting as a RADIUS proxy passthrough where a session is not created and the client's RADIUS messages are sent to an external AAA server.

How to Configure ISG as a RADIUS Proxy in Passthrough Mode

Enabling RADIUS Proxy Passthrough mode at Global Level

Perform this task to enable the RADIUS proxy passthrough mode globally.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa server radius proxy
5. mode pass-through
6. key [0 | 7] word
7. accounting method-list {method-list-name | default}
8. authentication method-list {method-list-name | default}
9. authentication port port-number
10. accounting port port-number
11. client {name | ip-address} [subnet-mask [vrfvrf-id]]
12. 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	aaa new-model **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	aaa server radius proxy **Example:** `Device(config)# aaa server radius proxy`	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	mode pass-through **Example:** `Device(config-locsvr-proxy-radius)# mode pass-through`	Enables ISG RADIUS proxy pass-through mode.

	Command or Action	Purpose
Step 6	key [0 | 7] word **Example:** `Device(config-locsvr-proxy-radius)# key radprxykey`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 7	accounting method-list {method-list-name | default} **Example:** `Device(config-locsvr-proxy-radius)# accounting method-list SVC_ACCT`	Specifies the server to which accounting packets from RADIUS clients are forwarded.
Step 8	authentication method-list {method-list-name | default} **Example:** `Device(config-locsvr-proxy-radius)# authentication method-list SVC_ACCT`	Specifies the server to which authentication packets from RADIUS clients are forwarded.
Step 9	authentication port port-number **Example:** `Device(config-locsvr-proxy-radius)# authentication port 1645`	Specifies the port on which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.
Step 10	accounting port port-number **Example:** `Device(config-locsvr-proxy-radius)# accounting port 1646`	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. • The default port is 1646.
Step 11	client {name | ip-address} [subnet-mask [vrfvrf-id]] **Example:** `Device(config-locsvr-proxy-radius)# client 1.1.1.1`	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS proxy client configuration mode.
Step 12	end **Example:** `Device(config-locsvr-radius-client)# end`	Exits the ISG RADIUS proxy client configuration mode and returns to privileged EXEC mode.

Enabling RADIUS Proxy Passthrough mode at Client Level

Perform this task to enable the RADIUS proxy passthrough mode for an individual client.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa server radius proxy
5. client {name | ip-address} [subnet-mask [vrfvrf-id]]

6. mode pass-through
7. key [0 | 7] word
8. accounting method-list {method-list-name | default}
9. authentication method-list {method-list-name | default}
10. authentication port port-number
11. accounting port port-number
12. 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	aaa new-model **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization and accounting(AAA) access control model.
Step 4	aaa server radius proxy **Example:** `Device(config)# aaa server radius proxy`	Enters Intelligent Services Gateway (ISG) RADIUS proxy server configuration mode.
Step 5	client {name | ip-address} [subnet-mask [vrfvrf-id]] **Example:** `Device(config-locsvr-proxy-radius)# client 1.1.1.1`	Specifies a RADIUS proxy client for which client-specific parameters can be configured, and enters RADIUS proxy client configuration mode.
Step 6	mode pass-through **Example:** `Device(config-locsvr-radius-client)# mode pass-through`	Enables ISG RADIUS proxy pass-through mode.
Step 7	key [0 | 7] word **Example:** `Device(config-locsvr-radius-client)# key radprxykey`	Configures the encryption key to be shared between ISG and RADIUS clients. • 0 specifies that an unencrypted key will follow. • 7 specifies a hidden key will follow.
Step 8	accounting method-list {method-list-name | default} **Example:** `Device(config-locsvr-radius-client)# accounting method-list SVC_ACCT`	Specifies the server to which accounting packets from RADIUS clients are forwarded.

	Command or Action	Purpose
Step 9	authentication method-list {method-list-name | default} **Example:** `Device(config-locsvr-radius-client)# authentication method-list SVC_ACCT`	Specifies the server to which authentication packets from RADIUS clients are forwarded.
Step 10	authentication port port-number **Example:** `Device(config-locsvr-radius-client)# authentication port 1645`	Specifies the port for which the ISG listens for authentication packets from RADIUS clients. • The default port is 1645.
Step 11	accounting port port-number **Example:** `Device(config-locsvr-radius-client)# accounting port 1646`	Specifies the port on which the ISG listens for accounting packets from RADIUS clients. • The default port is 1646.
Step 12	end **Example:** `Device(config-locsvr-radius-client)# end`	Exits the ISG RADIUS proxy client configuration mode and returns to privileged EXEC mode.

Verifying ISG RADIUS Proxy Passthrough Sessions

SUMMARY STEPS

1. enable
2. show radius-proxy statistics
3. end

DETAILED STEPS

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

Step 2	show radius-proxy statistics
	Example:
	`Device> show radius-proxy statistics`
	`Device> show radius-proxy statistics | include access request`
		Displays statistics of all RADIUS proxy sessions on the ISG.
		Note You can also use appropriate output modifiers to display a section of the statistics for all the ISG RADIUS proxy sessions based on the specification.

Step 3	end **Example:** `Device> end`	Returns to user EXEC mode.

Clearing ISG RADIUS Proxy Statistics

SUMMARY STEPS

1. enable
2. clear radius-proxy statistics
3. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	clear radius-proxy statistics **Example:** `Device> clear radius-proxy statistics`	Clears all ISG RADIUS proxy statistics.
Step 3	end **Example:** `Device> exit`	Returns to user EXEC mode.

Configuration Examples for Configuring ISG as RADIUS Proxy in Passthrough Mode

Example: Configuring Radius Proxy Passthrough Mode

The following example shows how to configure ISG as a RADIUS Proxy passthrough where the interface is configured with dual initiators. Here, an ISG session is not created for the client 10.0.0.2 as it is in passthrough mode whereas a session is created for the client 12.0.0.2 as session creation is triggered by the RADIUS proxy initiator.

```
aaa server radius proxy
message-authenticator ignore
!
client 10.0.0.2
mode pass-through
key radprxykey
accounting method-list SVC_ACCT
authentication port 1645
accounting port 1646

client 12.0.0.2
key radprxykey
accounting method-list SVC_ACCT
```

```
authentication method-list SVC_ACCT
authentication port 1647
accounting port 1648
```

Example: Verifying Radius Proxy Passthrough Mode

Use the **show radius-proxy statistics** command to verify that ISG is functioning in RADIUS proxy passthrough mode.

The following is a sample output from the **show radius-proxy statistics** command, showing information for both passthrough and non-passthrough clients.

```
Device#show radius-proxy statistics

 NON-PASSTHROUGH CLIENTS
 FROM:                  Client       ISG          AAA
Access Requests:          0           0            0
Access Accepts:           0           0            0
Access Rejects:           0           0            0
Access Challenges         0           0            0
Accounting Requests       0           0            0
Accounting Starts         0           0            0
Accounting Stops          0           0            0
Accounting Updates        0           0            0
Accounting Responses      0           0            0
Accounting ON/OFFS        0           0            0

 PASSTHROUGH CLIENTS
 FROM:                  Client       ISG          AAA
Access Requests:          48000       48000        0
Access Accepts:           0           48000        48000
Access Rejects:           0           0            0
Access Challenges         0           0            0
Accounting Requests       80000       80000        0
Accounting Starts         80000       0            0
Accounting Stops          0           0            0
Accounting Updates        0           0            0
Accounting Responses      0           0            80000
Accounting ON/OFFS        0           0            0
```

Additional References for ISG as RADIUS Proxy in Passthrough Mode

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference
ISG as RADIUS Proxy	"Configuring ISG as a RADIUS Proxy" module in the *Intelligent Services Gateway Configuration Guide*

Related Topic	Document Title
RADIUS configurations	"Configuring RADIUS" module in the *RADIUS Configuration Guide*
ISG Subscriber Service configurations	"Configuring ISG Subscriber Services" module in the *Intelligent Services Gateway Configuration Guide*
Command Lookup Tool	Command Lookup Tool

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

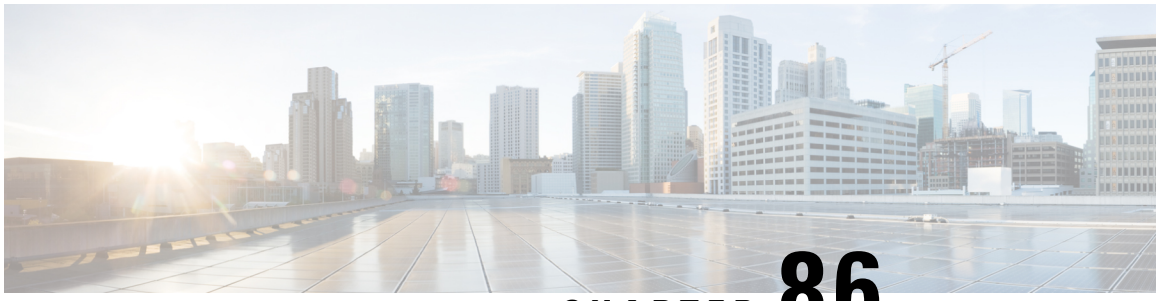
Feature Information for Configuring ISG as a RADIUS Proxy in Passthrough Mode

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 112: Feature Information for Configuring ISG as a RADIUS Proxy in Passthrough Mode

Feature Name	Releases	Feature Information
Configuring ISG as a RADIUS Proxy in Passthrough Mode		Configuring the ISG as a RADIUS Proxy in Passthrough Mode allows the Cisco Intelligent Services Gateway (ISG) acting as a RADIUS Proxy to direct all the RADIUS traffic from the client to the RADIUS server, without creating an ISG session. The following commands were introduced: **mode pass-thru** and **authentication method-list list-authen**.



CHAPTER 86

ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

The ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering feature allows the Intelligent Services Gateway (ISG) to perform the following:

- Allow the hotspot roaming subscriber to continue accessing the ISG services seamlessly.
- Filter RADIUS packets that are received by the RADIUS proxy server based on the attributes present in the packets.

Restrictions for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Restrictions for RADIUS Proxy Support for Hotspot Roaming

A subscriber is connected to an access point (AP1) that is connected to an Access Zone Router (AZR) (AZR1). The subscriber moves to a different AZR and moves back to a different access point (AP2) within AZR1. When the subscriber tries to reauthenticate with the same IP address that it had for AP1, ISG cannot determine that it is a new session with AP2 and terminates the session when the roaming timer expires.

Restrictions for RADIUS Proxy Support for Accounting Start Filtering

- Configuring RADIUS packet filtering in RADIUS proxy client configuration mode can cause negative impact on the number of RADIUS packets that ISG can process in a second and can bring down calls per second.
- A maximum of four filters can be applied to a single configuration.

Information About ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Hotspot Roaming Timer

When an Extensible Authentication Protocol (EAP)-authenticated subscriber moves from one hotspot to another (hotspot roaming), the subscriber authenticates against a new access point. ISG checks the following conditions to validate if the user has roamed from one hotspot to another:

- The IP address of the access point has changed.
- The user is authenticated.

If the reauthentication on hotspot roaming is successful, the ISG RADIUS proxy server saves the following data in the RADIUS proxy session context:

- The time of reauthentication.
- Authorization data that comes as part of the reauthentication.

If the reauthentication fails, ISG clears the session.

If reauthentication is successful, ISG receives an accounting-start request on the existing session from the new access point, with a different IP address. ISG creates a new RADIUS proxy session for the subscriber with a new IP address and provides seamless roaming by applying the services saved during reauthentication if the following conditions are satisfied:

- The time difference between the arrival of the accounting start request and the reauthentication request is less than the configured IP timer. For more information on IP timers, see the “Configuring ISG RADIUS Proxy Global Parameters” and the “Configuring ISG RADIUS Proxy Client-Specific Parameters” sections in the “Configuring ISG as a RADIUS Prox”y chapter.
- The subscriber is EAP-authenticated.

If the new session is created successfully, a roaming timer is started for the first session. Use the **timer roaming** command in RADIUS proxy server configuration and RADIUS proxy client configuration modes to configure the roaming timer. Once the cleanup timer expires, ISG clears the first session, and the second session remains as the only session for the subscriber.

If the subscriber moves back to the first hotspot before the roaming timer expires on the first session and reauthentication is successful, the roaming timer is stopped for the first session. A new roaming timer is initiated for the second session. If the reauthentication fails, the first session is cleared.

If ISG receives an accounting-stop request for the first session from the AZR to which the session belongs, before the roaming timer expires, the timer is stopped and the first session is cleared. The accounting-stop request is forwarded to the RADIUS server. The response from the RADIUS server is forwarded to the AZR.

If the subscriber roams between multiple hotspots, ISG creates multiple parallel sessions. All these sessions are maintained on ISG until the roaming timer associated with them expires. Only the session that is authenticated last is not associated with a roaming timer.

RADIUS Packet Filter Creation

The RADIUS filter consists of a filter structure and a CLI through which subscribers can configure the filter on RADIUS packets. When a packet is received by ISG, ISG reads the attributes in the packet and matches them with the attributes defined in the filter. Depending on the match criteria that are specified in the filter, ISG takes the defined action on the RADIUS packet.

To create a RADIUS packet filter, follow three steps:

1. Create the RADIUS filter with match criteria.
2. Get the list of standard IETF attributes or vendor-specific attributes from the RADIUS packet that is received.
3. Accept, reject, or ignore the RADIUS packets by applying the filter criteria.

How to Configure ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Configuring a Roaming Timer for the ISG RADIUS Proxy Session

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **timer roaming** *timer-value*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters 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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa server radius proxy** **Example:** `Device(config)# aaa server radius proxy`	Enters ISG RADIUS proxy server configuration mode.
Step 5	**timer roaming** *timer-value* **Example:** `Device(config-locsvr-proxy-radius)# timer roaming 60`	Configures a roaming timer for 60 seconds.
Step 6	**end** **Example:** `Device(config-locsvr-proxy-radius)# end`	Returns to privileged EXEC mode.

Configuring RADIUS Proxy Support for Accounting Start Filtering

The Accounting Start Filtering feature allows the creation of RADIUS packet filtering to filter packets that reach ISG. Based on the defined filter criteria, ISG performs certain actions on the RADIUS packet.

The RADIUS packet filter is created on ISG by defining the filter name and the match criteria in the **radius filter** command. The match criteria are applied to the attributes of the RADIUS packet. When you configure the **radius filter match-all** command, the filter is applied to the RADIUS packet only if all the attributes configured in the command match the attributes in the RADIUS packet. When you configure the **radius filter match-any** command, the filter is applied to the RADIUS packet if at least one attribute configured in the command matches the attributes in the RADIUS packet. The attributes to match are defined in RADIUS filter configuration mode.

In RADIUS filter configuration mode, you can specify a standard IETF RADIUS attribute or a vendor-specific RADIUS attribute. These attributes must match the attributes in the RADIUS packet so that the filter can be applied accordingly. The **match** command checks if the attribute is present in the packet, and the **matchnot** command checks if the attribute is not present in the packet.

Apply RADIUS filters to the RADIUS proxy server in order for the configuration to take effect. Apply RADIUS filters in RADIUS proxy server configuration mode and RADIUS proxy client configuration mode. If filters are applied in both modes, only the client mode configuration will take effect.

You can specify the type of RADIUS packets to which the filter should be applied using the **filter access** and **filter accounting** commands.

You can configure any one of the following three actions that the RADIUS proxy server should apply to the incoming RADIUS packets to complete the filtering process:

- **drop**—Drops the RADIUS packet.
- **ignore**—Forwards the packet to the RADIUS server, but does not apply any ISG-related features to the RADIUS packet.
- **ack**—Returns the access-accept response for the access packet and the accounting response for the accounting packet.

Perform the following tasks to configure a RADIUS packet filter and apply the filter criteria to RADIUS proxy.

Configuring a RADIUS Packet Filter

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius filter match-all** *name*
4. **match attribute** *att-type-number*
5. **matchnot vendor-type** *9*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius filter match-all** *name* **Example:** `Device(config)# radius filter match-all filter1`	Configures a RADIUS packet filter, defines the condition to filter RADIUS packets if all attributes match, and enters RADIUS filter configuration mode. • The filter condition is applied only after the attributes are defined in RADIUS filter configuration mode.
Step 4	**match attribute** *att-type-number* **Example:**	Configures a match condition.

	Command or Action	Purpose
	`Device(config-radius-filter)# match attribute 25`	
Step 5	**matchnot vendor-type** *9* **Example:** `Device(config-radius-filter)# matchnot vendor-type 9`	Configures a vendor-type match condition.
Step 6	**end** **Example:** `Device(config-radius-filter)# end`	Returns to privileged EXEC mode.

Applying RADIUS Filters to RADIUS Proxy Server or Client

Use the **filter** command in RADIUS proxy server configuration mode or RADIUS proxy client configuration mode to apply a RADIUS filter. If the RADIUS filter is configured in both these modes, only the filter configured in the client mode will be applied.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius proxy**
5. **filter access ack** *name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control model.

	Command or Action	Purpose
Step 4	**aaa server radius proxy** **Example:** `Device(config)# aaa server radius proxy`	Enters RADIUS proxy server configuration mode.
Step 5	**filter access ack** *name* **Example:** `Device(config-locsvr-proxy-radius)# filter access ack filter1`	Acknowledges the RADIUS packet for access requests.
Step 6	**end** **Example:** `Device(config-locsvr-proxy-radius)# end`	Returns to privileged EXEC mode.

Configuration Examples for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Example: Configuring a Roaming Timer for an ISG RADIUS Proxy Session

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# timer roaming 60
```

Example: Configuring a RADIUS Packet Filter

Use the following example along with the example given in the "Example: Applying RADIUS Packet Filters to RADIUS Proxy Server, on page 1260" section to configure a RADIUS packet filter for the RADIUS proxy server.

The following example shows how to create the RADIUS packet filter, filter1, and define the matching conditions:

```
Device> enable
Device# configure terminal
Device(config)# radius filter match-all filter1
Device(config)# match attribute 25
Device(config)# match attribute 100
Device(config)# matchnot vendor-type 100
```

Example: Applying RADIUS Packet Filters to RADIUS Proxy Server

Use the following example along with the example given in "Example: Configuring a RADIUS Packet Filter, on page 1259" section to configure a RADIUS packet filter for the RADIUS proxy server.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius proxy
Device(config-locsvr-proxy-radius)# filter access ack filter1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

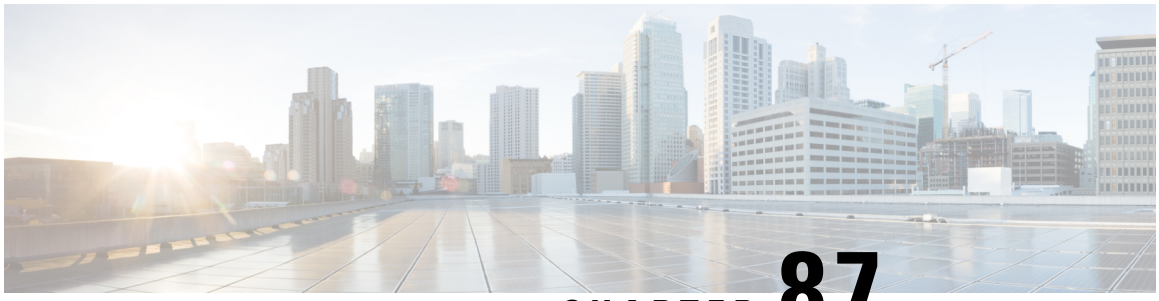
Feature Information for ISG RADIUS Proxy Support for Mobile Users: Hotspot Roaming and Accounting Start Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 113: Feature Information for ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering

Feature Name	Releases	Feature Information
ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering	Cisco IOS XE Release 3.5S	The ISG RADIUS Proxy Support for Mobile Users—Hotspot Roaming and Accounting Start Filtering feature allows you to configure hotspot roaming and RADIUS packet filtering for RADIUS proxy sessions. The following commands were introduced or modified: **filter (radius-proxy)**, **match (radius-filter)**, **matchnot (radius-filter)**, **radius filter**, and **timer (ISG RADIUS proxy)**.



CHAPTER 87

Walk-By User Support in ISG

The Walk-By User Support in ISG feature enables the Cisco Intelligent Services Gateway (ISG) to handle unauthenticated sessions from neighboring devices that do not intend to use the ISG service. These sessions, called walk-by sessions or lite sessions, may be triggered by various initiators.

With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session.

This module describes how to create and apply a default policy for default sessions to enable the Walk-By User Support in ISG feature.

Prerequisites for Walk-By User Support for PWLANs in ISG

Your implementation of the Cisco software image must support authentication, authorization, and accounting (AAA) and Intelligent Services Gateway (ISG).

Restrictions for Walk-By User Support for PWLANs in ISG

- IPv6 sessions are not supported.
- Only Layer 4 Redirect (L4R), Port-Bundle Host Key (PBHK), and service virtual routing and forwarding (VRF) features are supported. The L4R feature for walk-by session supports only 16 translation entries.
- Lite sessions do not support prepaid, accounting, quality of service (QoS), timers, or RADIUS-timeout features.

Information About Walk-By User Support for PWLANs in ISG

Default Sessions

A default session is a template session that is used as a reference by lite sessions created for walk-by subscribers on a given interface. When an edge device connects to an open service set ID (SSID) in a public wireless LAN (PWLAN) environment a lite session is created on the Intelligent Services Gateway (ISG). Each lite session applies the session start services defined in the default policy configured for the default session. Only one default session can be configured on each device interface. The default policy defines the default session start services and features to be used as a template for the lite session.

Lite Sessions or Walk-By Sessions

In most public wireless LAN (PWLAN) setups, a high percentage of Intelligent Services Gateway (ISG) sessions are unauthenticated sessions from wireless devices that do not use the PWLAN service. These sessions are called walk-by sessions or lite sessions, and users that use these sessions are called walk-by users. Walk-by sessions consume a significant amount of CPU, memory and other physical resources of the ISG router. This resource utilization may lead to an increase in the number of ISG devices that are required for a given PWLAN deployment.

A lite session inherits the session start services applied for the default session. Lite sessions are created on ISG to support walk-by users and optimize resource usage. Each lite session is associated with an individual timer that specifies the duration for which the session can utilize PWLAN services while remaining unauthenticated. If these lite sessions remain unauthenticated even after the timer expires, these sessions are deleted from ISG.

Lite sessions are also created when dedicated sessions fail authentication.

Dedicated Sessions

A dedicated or regular session is a full-fledged Intelligent Services Gateway (ISG) subscriber session. All subscriber sessions that are authenticated cause the creation of dedicated sessions on ISG. The policy manager of ISG decides whether to create a complete session context (a dedicated session) or a minimal session context (a lite session).

Note ISG provides high availability support for converted (lite to dedicated) unclassified and DHCPv4 sessions.

Supported Triggers

Walk-by sessions can be created through any of the following session initiators:

- Packet trigger: Here the session creation is triggered by a subscriber's IP packet having an unclassified IP address or MAC address.
- RADIUS proxy: This trigger is commonly used in PWLAN deployments where ISG acts as a RADIUS proxy. Here, the session creation is triggered by the subscriber's RADIUS packets.

- DHCP: This trigger is another SIP used in a few PWLAN deployments. Here, the session creation is triggered by the subscriber's DHCP control packets.
- EoGRE walkby: When ISG is configured for EoGRE, DHCP control packets and unclassified MAC packets on the EoGRE interface trigger session creation on ISG.

Session Limit

The total number of sessions supported on ISG is 128,000. Currently, ISG can support 128,000 lite sessions and 64,000 converted sessions. ISG can also now support 64,000 tunnel endpoints.

How to Configure Walk-By User Support for PWLANs in ISG

Creating and Enabling a Default Policy for a Default Session

Perform this task to create and enable a default policy for a default session on an interface. Each interface can have only one default policy.

A default session is set up to optimize the creation of Intelligent Services Gateway (ISG) sessions for walk-by users. The default session serves as a template that is used by lite sessions for walk-by users. The default policy contains session start services only to which all lite sessions refer. A default policy has the following two functions:

- Identify users who qualify for lite session optimization.
- Identify services or features that need to be applied on default sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **service local**
5. **ip portbundle**
6. **exit**
7. **class-map type traffic match-any** *class-map-name*
8. **match access-group** {**input** | **output**} {*access-list-number* | **name** *access-list-name*}
9. **exit**
10. **policy-map type service** *policy-map-name*
11. [*priority*] **class type traffic** {*class-map-name* | **default** {**in-out** | **input** | **output**}}
12. **redirect to group** {*server-group-name* | **ip** *server-ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]]
13. **exit**
14. **exit**
15. **policy-map type control** *policy-map-name*
16. **class type control** {*control-class-name* | **always**} [**event session-start**]
17. *action-number* **service-policy type service name** *policy-map-name*

18. *action-number* **service-policy type service name** *policy-map-name*
19. *action-number* **set-timer** *name-of-timer minutes*
20. **exit**
21. **exit**
22. **interface** *type number*
23. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
24. **service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]}
25. **end**
26. **show running-config interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service PBHK`	Configures a service policy map, and enters service policy-map configuration mode.
Step 4	**service local** **Example:** `Device(config-service-policymap)# service local`	Specifies the local termination service in the ISG service policy map.
Step 5	**ip portbundle** **Example:** `Device(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key (PBHK) feature for the service.
Step 6	**exit** **Example:** `Device(config-service-policymap)# exit`	Returns to global configuration mode.
Step 7	**class-map type traffic match-any** *class-map-name* **Example:** `Device(config)# class-map type traffic match-any ALLTRAFFIC`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class, and enters traffic class-map configuration mode.
Step 8	**match access-group** {**input** | **output**} {*access-list-number* | **name** *access-list-name*} **Example:**	Configures the match criteria for an ISG traffic class map on the basis of the specified access control list (ACL).

	Command or Action	Purpose
	`Device(config-traffic-classmap)# match access-group input 100`	
Step 9	**exit** **Example:** `Device(config-traffic-classmap)# exit`	Exits traffic class-map configuration mode.
Step 10	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service L4R`	Configures another service policy map, and enters service policy-map configuration mode.
Step 11	[*priority*] **class type traffic** {*class-map-name* | **default** {**in-out** | **input** | **output**}} **Example:** `Device(config-service-policymap)# class type traffic ALLTRAFFIC`	Associates a previously configured ISG traffic class map with a service policy map, and enters service policy-map traffic class configuration mode.
Step 12	**redirect to group** {*server-group-name* | **ip** *server-ip-address* [**port** *port-number*]} [**duration** *seconds* [**frequency** *seconds*]] **Example:** `Device(config-service-policymap-class-traffic)# redirect to group PORTAL`	Redirects ISG Layer 4 traffic to a specified server or server group.
Step 13	**exit** **Example:** `Device(config-service-policymap-class-traffic)# exit`	Returns to service policy-map configuration mode.
Step 14	**exit** **Example:** `Device(config-service-policymap)# exit`	Returns to global configuration mode.
Step 15	**policy-map type control** *policy-map-name* **Example:** `Device(config)# policy-map type control DefRULE`	Creates or modifies a default control policy map, which is used to define a control policy, and enters control policy-map configuration mode.
Step 16	**class type control** {*control-class-name* | **always**} [**event session-start**] **Example:** `Device(config-control-policymap)# class type control always event session-start`	Specifies a control class for which actions are configured and enters control policy-map class configuration mode.
Step 17	*action-number* **service-policy type service name** *policy-map-name* **Example:**	Activates the specified ISG service.

	Command or Action	Purpose
	`Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK`	
Step 18	*action-number* **service-policy type service name** *policy-map-name* **Example:** `Device(config-control-policymap-class-control)# 20 service-policy type service name L4R`	(Optional) Activates another specified ISG service.
Step 19	*action-number* **set-timer** *name-of-timer minutes* **Example:** `Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1`	Starts a named policy timer. • Expiration of the timer initiates the timed-policy-expiry event.
Step 20	**exit** **Example:** `Device(config-control-policymap-class-control)# exit`	Returns to control policy-map configuration mode.
Step 21	**exit** **Example:** `Device(config-control-policymap)# exit`	Returns to global configuration mode.
Step 22	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/4`	Specifies an interface and enters interface configuration mode.
Step 23	**service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]} **Example:** `Device(config-if)# service-policy type control default DefRULE`	Applies a default control policy on the interface.
Step 24	**service-policy type control** {*policy-map-name* | **default** [*def-policy-map-name*]} **Example:** `Device(config-if)# service-policy type control RegRULE`	Applies a regular control policy on the interface.
Step 25	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 26	**show running-config interface** *type number* **Example:** `Device# show running-config interface GigabitEthernet 0/0/4`	(Optional) Displays the running configuration for a specific interface.

Configuration Examples for Walk-By User Support for PWLANs in ISG

Example: Creating and Enabling a Default Policy for a Default Session

The following example shows how to create and enable a default policy named DefRULE on the Gigabit Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# policy-map type service PBHK
Device(config-service-policymap)# service local
Device(config-service-policymap)# ip portbundle
Device(config-service-policymap)# exit
Device(config)# class-map type traffic match-any ALLTRAFFIC
Device(config-traffic-classmap)# match access-group input 100
Device(config-traffic-classmap)# exit
Device(config)# policy-map type service L4R
Device(config-service-policymap)# class type traffic ALLTRAFFIC
Device(config-service-policymap-class-traffic)# redirect to group PORTAL
Device(config-service-policymap-class-traffic)# exit
Device(config-service-policymap)# exit
Device(config)# policy-map type control DefRULE
Device(config-control-policymap)# class type control always event session-start
Device(config-control-policymap-class-control)# 10 service-policy type service name PBHK
Device(config-control-policymap-class-control)# 20 service-policy type service name L4R
Device(config-control-policymap-class-control)# 30 set-timer UNAUTH 1
Device(config-control-policymap-class-control)# exit
Device(config-control-policymap)# exit
Device(config)# interface GigabitEthernet 0/0/4
Device(config-if)# service-policy type control default DefRULE
Device(config-if)# service-policy type control RegRULE
Device(config-if)# end
```

The following sample output from the **show running-config interface** command displays the policies configured on the Gigabit Ethernet interface. The default policy configured for default sessions on the Gigabit Ethernet interface is DefRULE, and the regular policy configured for dedicated sessions on the Gigabit Ethernet interface is RegRULE.

```
Device# show running-config interface GigabitEthernet 0/0/4

Building configuration...

Current configuration : 318 bytes
!
interface GigabitEthernet0/0/4
ip address 192.0.2.1 255.255.255.0
negotiation auto
service-policy type control default DefRULE
service-policy type control RegRULE
ip subscriber routed
  initiator unclassified ip-address
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

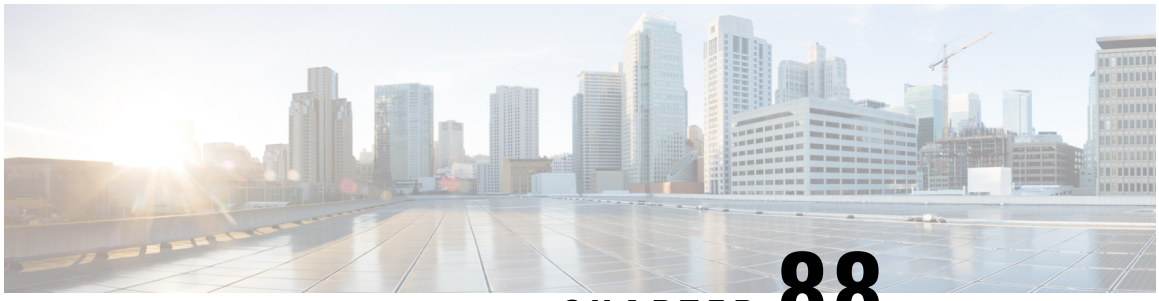
Feature Information for Walk-By User Support for PWLANs in ISG

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 114: Feature Information for Walk-By User Support for PWLANs in ISG

Feature Name	Releases	Feature Information
Walk-By User Support for PWLANs in ISG	Cisco IOS XE Release 3.7S	The Walk-By User Support for PWLANs in ISG feature enables the Intelligent Services Gateway (ISG) that is configured as a RADIUS proxy to handle unauthenticated sessions from wireless devices that do not use the public wireless LAN (PWLAN) service. These sessions are called walk-by sessions. With the implementation of this feature, unauthenticated users are assigned lite sessions based on the default session. These lite sessions optimize resource usage because they enable the walk-by user to use only session start services mentioned in the default policy configured for the default session. The following commands were introduced or modified: **clear subscriber lite-session**, **clear subscriber session**, **debug subscriber lite-session errors**, **debug subscriber lite-session events**, **service-policy type control**, **show subscriber default-session**, and **show subscriber statistics**.
Walkby session support on EoGRE interface	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support walk-by sessions over EoGRE interfaces
HA support for converted (lite to dedicated) sessions	Cisco IOS XE Release 3.13.1S	This feature enables the Intelligent Services Gateway (ISG) to support high availability for converted (lite to dedicated) sessions.



CHAPTER 88

ISG L2 Subscriber Roaming

Subscriber roaming is common in wireless deployments. The ISG L2 Subscriber Roaming feature supports simple IP subscribers connecting to the Cisco Intelligent Services Gateway (ISG) when the subscriber device roams between interfaces, VLANs, or VRFs. This module describes how to configure Layer 2 roaming for simple IPv4 ISG subscribers.

Restrictions for ISG L2 Subscriber Roaming

- Roaming is not supported for dual-stack sessions.
- Roaming is not supported for walk-by subscribers.
- Roaming between interfaces configured with different initiators are not supported.

Information About ISG L2 Subscriber Roaming

ISG Subscriber Roaming

Most devices used in wireless deployments are handheld ones like mobile phones and tablets. It is possible that the same subscriber connects to the Cisco ISG via different access points of the service provider. However, these access points may not always be connected to the ISG over the same VLAN or VRF.

Sometimes, a subscriber with an existing ISG session through a VLAN or VRF, reconnects to the ISG through another VLAN or VRF via a different access point. It is also possible that the VLAN or VRF does not change after the subscriber connects to the access point through the ISG via different physical interfaces or sub-interfaces. This behavior where there is a change in the SSID or access point for a given subscriber is called roaming.

Hence, a roaming subscriber is one who after moving between access points resumes the existing ISG session when it reappears on a new ISG interface.

However, a reconnect subscriber is one who gets a new ISG session when it reappears on the same or different interface. Sometimes, a subscriber who sends a DHCP Discover Packet may also be termed as a reconnect subscriber irrespective of whether it has an existing ISG session or not.

ISG L2 Roaming Events

L2 roaming is now automatically enabled on ISG. When an L2-connected subscriber roams, there may be a change in the session's key parameters. These parameters called session keys are listed below:

- IP Address
- VRF
- Subnet

Note This is applicable to DHCP deployments mostly.

- Initiator
- Control policy

When ISG receives a roaming trigger, it performs one of the following actions on the existing subscriber session:

- Update: When the session keys do not change, ISG updates the subscriber to a new access interface.

  The accounting interim records are sent to the RADIUS server with the updated interface details. Re-authentication may not happen.

- Reconnect: When the session keys change, ISG removes the existing session and re-creates a new subscriber session.

  The control policy is re-applied and the subscriber may be subjected to re-authorization.

- No change: When ISG receives DHCP control packets where ISG is neither a DHCP server nor a relay, ISG does not modify the existing session.

  A session update or reconnect occurs only if the subscriber sends data packets.

ISG L2 Roaming Deployments

Some of the deployments that L2 roaming is currently supported on are listed below:

- Unclassified MAC (External DHCP server)
- DHCP subscribers (DHCP relay)
- DHCP subscribers (DHCP server)
- Hybrid (DHCP with unclassified MAC)

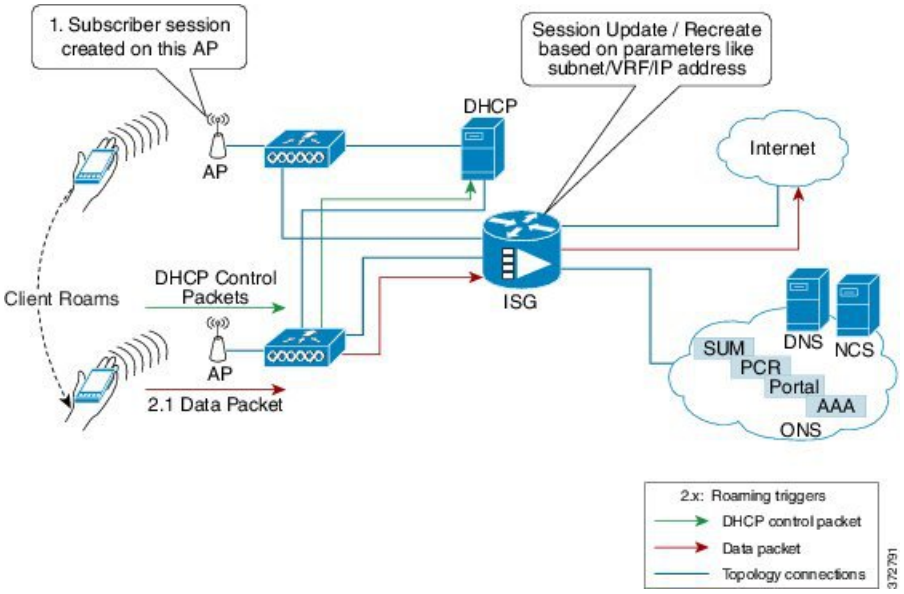
Unclassified MAC (External DHCP server)

For the external DHCP server model, ISG sessions are mainly created by unclassified packets, where the session identifiers will be the MAC address and IP address. The roaming triggers for this model are listed below:

Table 115: Simple IP L2-Connected Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP control packets (DHCP Discover, DHCP Request, Init Bootp)	No
Data packets	Yes

Figure 59: Simple IP L2-Connected Unclassified MAC Roaming



DHCP subscribers (DHCP relay)

For the DHCP relay model, the ISG sessions are mainly created by DHCP control packets. Here, the ISG relays these packets to the DHCP server and forwards the response received from the server back to the client. In this scenario, the subscriber that has roamed to a new interface may trigger one of the following session initiator packets:

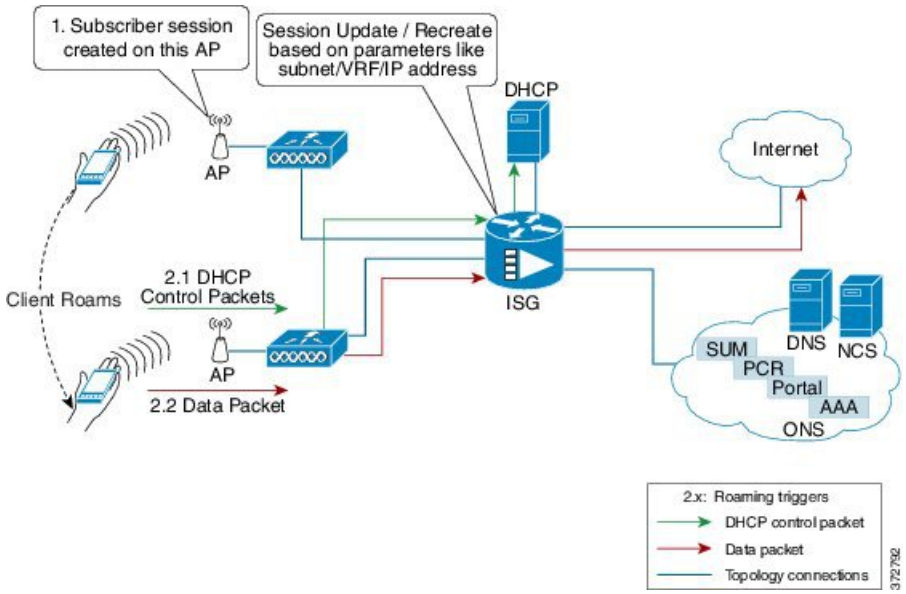
- Data packet if the subscriber has an existing IP address
- DHCP Renew control packet if the IP address needs to be renewed
- DHCP Discover control packet

The roaming triggers for the DHCP relay deployment are listed below:

Table 116: Simple IP L2-Connected (Dual Initiator) DHCP Relay with Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP Control Packets (DHCP Discover, DHCP Request, Init Bootp)	Yes
Data Packets	Yes

Figure 60: Simple IP L2-Connected (Dual Initiator) DHCP Relay with Unclassified MAC Roaming



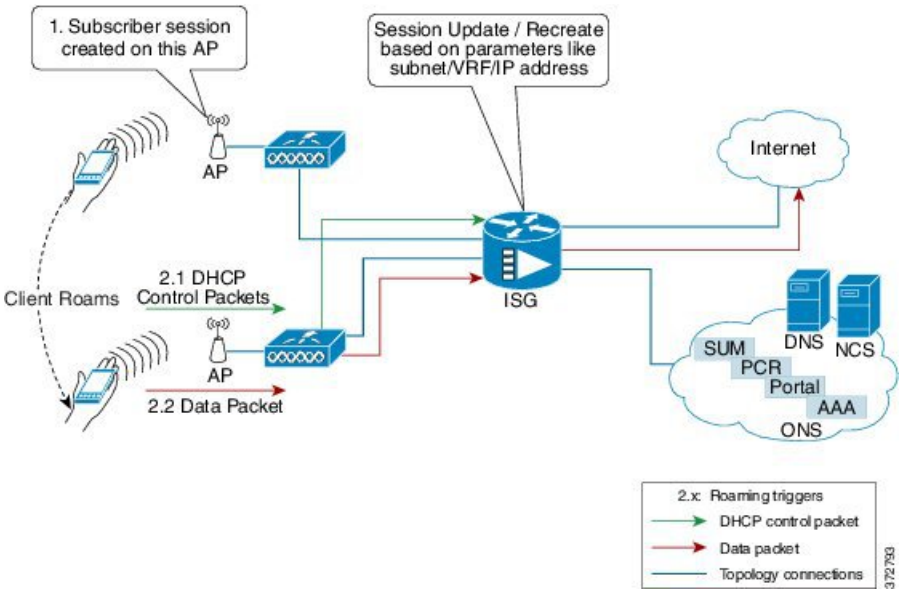
DHCP subscribers (DHCP server)

For the DHCP server deployment, ISG acts as a DHCP server. The roaming triggers for this model are listed below:

Table 117: Simple IP L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP Control Packets (DHCP Discover, DHCP Request, Init Bootp)	Yes
Data Packets	Yes

Figure 61: Simple IP L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC Roaming



Hybrid (DHCP with unclassified MAC)

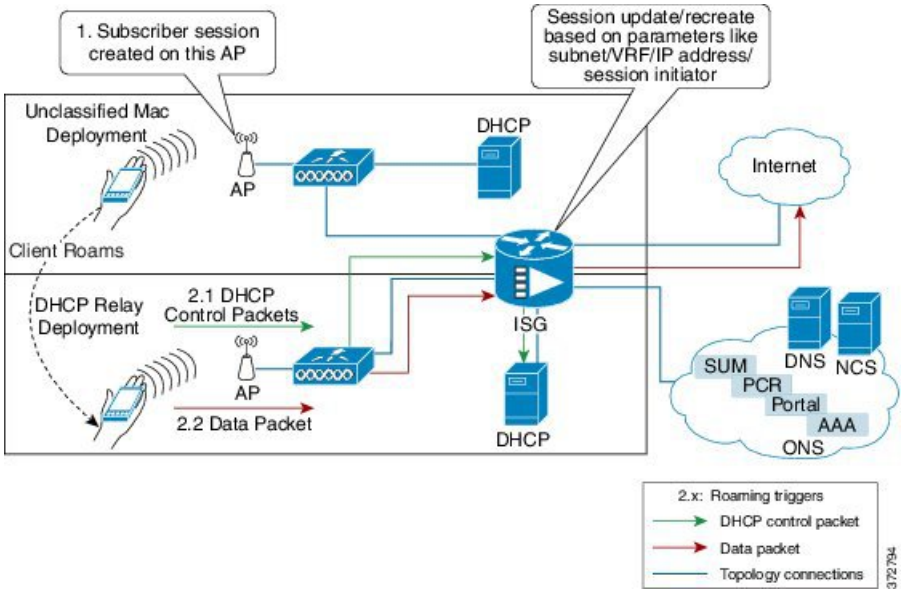
For the L2-connected hybrid model, the roaming triggers are listed below:

Table 118: Simple IP L2-Connected Hybrid (DHCP with unclassified MAC) Roaming Triggers

Packets	Roaming Trigger
GARP/ARP	No
DHCP control packets (DHCP Discover, DHCP Request, Init Bootp)	Yes [11]
Data packets	Yes

[11] DHCP control packets are considered as roaming triggers when the subscriber moves from unclassified MAC to DHCP deployments.

Figure 62: Simple IP L2-Connected Hybrid (DHCP with unclassified MAC) Roaming



ISG L2 Roaming Behavior

Table 119: Roaming behavior in ISG

Deployment Type	Client roams with different roaming triggers		Client roams and with changed network conditions	ISG Roaming Behavior	Client/System Behavior
	Packet	Roaming Trigger			
L2-connected unclassified MAC	GARP/ ARP	No	1. IP Address 2. Subnet 3. VRF 4. Control Policy	1. Session recreate 2. Session update 3. Session recreate 4. Session recreate	1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	No			
	Data packet	Yes			

Deployment Type	Client roams with different roaming triggers		Client roams and with changed network conditions	ISG Roaming Behavior	Client/System Behavior
	Packet	Roaming Trigger			
L2-connected (Dual Initiator) DHCP Relay with Unclassified MAC	GARP/ ARP	No	1. IP Address 2. Subnet 3. VRF 4. Control Policy	1. Session recreate. 2. Session update/recreate [12] 3. Session recreate. 4. Session recreate.	1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	Yes			
	Data packet	Yes			
L2-Connected (Dual Initiator) DHCP Server with Unclassified MAC	GARP/ ARP	No	1. IP Address 2. Subnet 3. VRF 4. Control Policy	1. Session recreate. 2. Session update/recreate.[13] 3. Session recreate 4. Session recreate	1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized.
	DHCP control packets	Yes			
	Data packet	Yes			
L2-Connected (Hybrid) DHCP Relay or Server with Unclassified MAC	GARP/ ARP	No	1. IP Address 2. Subnet 3. VRF 4. Control Policy 5. Initiator	1. Session recreate 2. Session update/recreate [14] 3. Session recreate 4. Session recreate 5. Session recreate	1. Client will be re-authorized. 2. Interim accounting record will be sent. 3. Client will be re-authorized. 4. Client will be re-authorized. 5. Client will be re-authorized.
	DHCP control packets	Yes (based on network conditions)			
	Data packet	Yes			

[12] DHCP control packets may trigger session recreate.
[13] DHCP control packets may trigger session recreate.
[14] Based on initiator, the session may be updated or recreated.

How to Configure ISG L2 Subscriber Roaming

Enabling Roaming for Simple IP Subscribers

Depending upon network design, subscribers may roam between interfaces, VLANs or VRFs.

Note Simple IP subscriber roaming is enabled by default. Hence, the **ip subscriber l2-roaming** command need not be configured to support roaming.

Configuration Examples for ISG L2 Subscriber Roaming

Example: Verifying L2 Roaming on ISG

Use the **show ip subscriber mac** *mac_address* command to verify that the ISG subscriber has successfully roamed to a new interface.

The following are sample outputs from the **show ip subscriber mac** *mac_address* command where the subscriber's session is updated due to roaming. On comparing the access interface parameter in both the outputs, you can see that it has changed indicating that the subscriber has roamed.

Before Roaming

```
Device# show ip subscriber mac aabb.cc01.9000

IP subscriber: aabb.cc01.9000, type connected, status up
  display uid: 1, aaa uid: 12
  segment id: 4098, session hdl: 0xF4000001, shdb: 0x3E000001
  session initiator: unclassified traffic
  access interface: Ethernet0/0.10                          # Note access interface
  access address: 1.1.1.2
  service address: 1.1.1.2
  status: IPv4 - Up  IPv6 - Down
  conditional debug flag: 0x0
  control plane state: connected, start time: 00:00:04
  data plane state: connected, start time: 00:00:04
  arp entry: 1.1.1.2, Ethernet0/0.10
  forwarding statistics:
    packets total: received 8, sent 7
    bytes total: received 944, sent 798
    packets dropped: 0, bytes dropped: 0
  hardware forwarding statistics:
    packets total: received 0, sent 0
    bytes total: received 0, sent 0
```

After Roaming

```
Device# show ip subscriber mac aabb.cc01.9000
```

```
IP subscriber: aabb.cc01.9000, type connected, status up
  display uid: 1, aaa uid: 12
  segment id: 4098, session hdl: 0xF4000001, shdb: 0x3E000001
  session initiator: unclassified traffic
  access interface: Ethernet0/0.20                      # Change in access interface
  access address: ::
  service address: ::
  access address: 1.1.1.2
  service address: 1.1.1.2
  status: IPv4 - Up  IPv6 - Down
  conditional debug flag: 0x0
  control plane state: connected, start time: 00:00:52
  data plane state: connected, start time: 00:00:52
  arp entry: 1.1.1.2, Ethernet0/0.20
  route: 1.1.1.2 -> Ethernet0/0.20
  forwarding statistics:
    packets total: received 18, sent 17
    bytes total: received 2124, sent 1938
    packets dropped: 0, bytes dropped: 0
  hardware forwarding statistics:
    packets total: received 0, sent 0
    bytes total: received 0, sent 0
```

Additional References for ISG L2 Subscriber Roaming

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

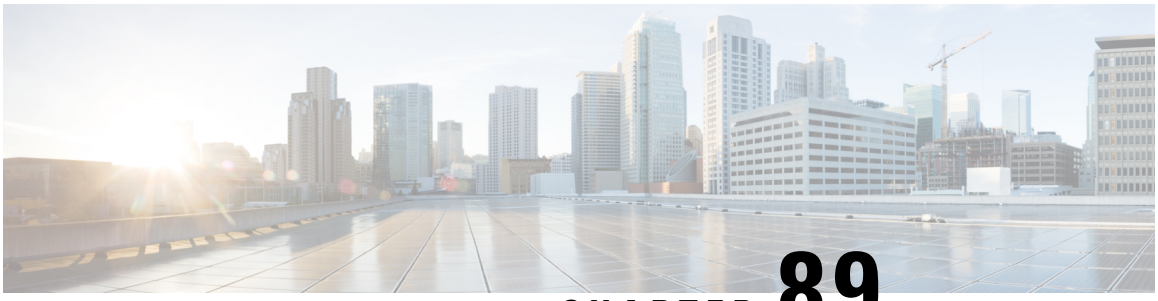
Feature Information for ISG L2 Subscriber Roaming

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 120: Feature Information for ISG L2 Subscriber Roaming

Feature Name	Releases	Feature Information
ISG L2 Subscriber Roaming	Cisco IOS XE Release 3.12S	Subscriber roaming is common in wireless deployments. The ISG L2 Subscriber Roaming feature supports simple IP subscribers connecting to the Cisco Intelligent Services Gateway (ISG) when the device roams between interfaces, VLANs or VRFs. The following command was deprecated: **ip subscriber l2-roaming**.



CHAPTER 89

Configuring RADIUS-Based Policing

The RADIUS-Based Policing feature enables Intelligent Services Gateway (ISG) to make automatic changes to the policing rate of specific sessions and services.

Prerequisites for RADIUS-Based Policing

You must configure all traffic classes on the ISG before referencing the classes in policy maps.

You must configure and apply QoS policy maps on the ISG before the ISG can construct and apply an ANCP-based dynamic service policy.

Restrictions for RADIUS-Based Policing

- Per-service policing cannot be configured on the class-default class at the parent level of a hierarchical policy. You can configure per-service policing on class-default classes at the child or grandchild level.
- Transient policies are not visible in the running-configuration file. Only the original policy configuration is visible.
- The parameterized Access Control List (pACL) name is limited to 80 characters. The pACL name is formed by concatenating the ACL entries in the RADIUS CoA or Access-Accept message to the ACL name configured on the ISG. If the pACL name exceeds 80 characters the parameterization operation fails and an error message displays. For a CoA message, the ISG also sends a negative Ack (Nack) response to the RADIUS server.
- The RADIUS-Based Policing feature is supported only on PPP Termination and Aggregation (PTA) sessions in Cisco IOS Release XE 3.1 and earlier releases; it is supported on L2TP access concentrator (LAC) or L2TP network server (LNS) sessions in Cisco IOS Release XE 3.2 and later releases.

- If there is a concatenated service-activation push, QoS policies are applied first and then service activation occurs. If a concatenated service activation fails, any QoS policies applied are not rolled back.
- Ensure that the classmap name specified for a policy-map configuration used to create pACL and class-map does not contain an hyphen (-) character.

Information About RADIUS-Based Policing

RADIUS Attributes

RADIUS communicates with ISG by embedding specific attributes in Access-Accept and change of authentication (CoA) messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services and to modify the active quality of service (QoS) policy applied to a session. The RADIUS server determines the new shaping or policing rate based on vendor-specific attributes (VSAs) configured in a subscriber's user profile on RADIUS and on the Advanced Node Control Protocol (ANCP)-signaled rate received from ISG.

After receiving the Access-Accept or CoA message, ISG copies the original policy map applied to the session and changes the shaping or policing rate of the copied, transient policy as indicated by RADIUS. ISG does not change the shaping rate of the original policy. After changing the transient policy, ISG applies the transient policy to the subscriber service.

The following sections describe the RADIUS attributes used in RADIUS-based policing:

RADIUS Attributes 250 and 252

RADIUS uses attribute 250 in Access-Accept messages and attribute 252 in CoA messages to activate and deactivate parameterized services. ISG services are configured locally on the ISG device; RADIUS sends only the service name.

Attributes 250 and 252 have the following syntax for service activation:

Access-Accept Messages

```
250 "Aservice(parameter1=value,parameter2=value,...)"
```

CoA Messages

```
252 0b "service(parameter1=value,parameter2=value,...)"
```

RADIUS uses only Attribute 252 in a CoA message when deactivating a service. RADIUS sends the same information in Attribute 252 that was used for service activation, except that service deactivation uses 0c in the syntax instead of the 0b parameter used for service activation.

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

VSA 252 has the above syntax for service deactivation.

Cisco VSA 1

RADIUS uses a vendor-specific attribute (VSA) 1 command to modify the active QoS policy on a session. This VSA has the following format:

```
av-pair = "policy-type=command 9 parameter1 ,...,parametern"
```

Use the following Cisco VSA 1 format to add and remove classes and QoS actions to and from the QoS policy that is currently active on a session:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

Before the ISG can construct a policy using the policing parameters specified in the RADIUS message, a QoS policy must be active on the session. If a QoS policy is not active in the specified direction, the ISG does not create the policy.

When implementing the changes specified in the Cisco VSA, the ISG does not make the changes to the originally configured QoS policy on the ISG device. Instead, the ISG copies the active QoS policy for the session and then makes the required changes to the policy copy, which is referred to as a *transient policy* . The originally configured QoS policy on the ISG device is not changed.

The following sections describe the Cisco VSA 1 commands used to automatically modify policing parameters of active policies:

Add-Class Primitive

To add or modify QoS actions to a traffic class, use the add-class primitive. This attribute has the following format:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
```

- *target* field—Indicates the QoS policy to be modified. The only valid value for this field is sub, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- *class-list* field—A list of class names enclosed in parentheses that identifies the traffic class to which the specified QoS action applies. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following class list identifies the class named “voip”, which gets added to a nested policy. The VoIP class is configured in a nested child policy that is applied to the parent class-default class.

```
(class-default, voip)
```

ISG Configuration

```
policy-map child
 class voip
 police 8000
policy-map parent
 class class-default
 service-policy child
```

The following class list specifies the voip-2 class, which is configured in a nested policy that is applied to the voip-aggregate class of another nested child policy. The policy containing the voip-aggregate class is in turn nested under the class-default class of the QoS policy attached to the target session.

```
(class-default, voip-aggregate, voip-2)
```

MSQ Configuration

```
policy-map child2
 class voip-2
 police 8000
policy-map child1
 class voip-aggregate
 police 20000
 service-policy child2
policy-map parent
 class class-default
 shape 512000
 service-policy child1
```

The *qos-actions-list* field indicates a QoS action such as police, followed by the action parameters enclosed in parentheses and separated by commas. For example, the following sample configuration specifies the police action and defines the parameters *bps*, *burst-normal*, *burst-max*, *conform-action*, *exceed-action*, and *violate-action*. Parentheses enclose the action parameters.

```
(voip-aggregate police(200000,9216,0,transmit,drop,drop))
```

Note The example shows a double-parenthesis at the end, because the syntax of the VSA specifies enclosure of the target, class-list, and qos-actions-list in parentheses.

Remove-Class Primitive

To remove traffic classes and QoS actions defined in the active QoS policy on a session, use the remove-class primitive. This attribute has the following format:

```
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

- target field—Indicates the QoS policy to be modified. The only valid value for this field is sub, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- class-list field—A list of class names enclosed in parentheses that identifies the class or classes to be removed. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following VSA1 attribute removes the Bronze class and all associated QoS policy actions from the nested child policy that is applied to the parent class-default class:

```
qos-policy-out=remove-class(sub,(class-default,Bronze))
```

When you remove a traffic class from a QoS policy, all of the attributes for the class are also removed. To re-add the class with the same attributes, you must reissue the add-class RADIUS attribute and provide the required parameters and values.

Parameterized QoS Policy as VSA 1

Multiple complex strings in a CoA message are not supported because they do not display the correct behavior of VSA 1, as shown in the following example:

```
vsa cisco 250 S152.1.1.2
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct1(1)((c-d,tv)1(10000))"
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct(1)((c-d,voip)1(10000))"
```

In the example:

- All services are enabled on target.
- Parameterized QoS policy in the second command syntax is not echoed in the ISG service.
- Parameterized QoS policy in the first command syntax is echoed.

Parameterization of QoS ACLs

The Parameterization of QoS Access Control Lists (ACLs) feature supports multiple ISG and QoS parameterized services in a single Access-Accept or CoA message. This feature allows the authentication, authorization, and accounting (AAA) device to change parameters dynamically.

HA Support for RADIUS-Based Policing

The ISG Policy HA and RADIUS-Based Policing HA feature adds stateful switchover (SSO) and In Service Software Upgrade (ISSU) support to ISG RADIUS-Based Policing for QoS parameterization that is configured through template services.

For information about modifying QoS policy maps by using template services, see the "QoS Policy Accounting" module in the QoS: Policing and Shaping Configuration Guide, Cisco IOS XE Release 3S .

For information about configuring High Availability (HA) on the ISG router, see the High Availability Configuration Guide, Cisco IOS XE Release 3S .

How to Configure RADIUS-Based Policing

Configuring per-Session Shaping

Configuring a QoS Policy with Shaping on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]

6. **service-policy** *policy-map-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a policy-map and enters QoS policy-map configuration mode.
Step 4	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Modifies the class-default traffic class and enters QoS policy-map class configuration mode.
Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the child policy map to the parent class-default class. • *policy-map-name*—Name of the child policy map.
Step 7	**end** **Example:** `Router(config-pmap-c)# end`	Exits QoS policy-map class configuration mode and returns to privileged EXEC mode.

Configuring per-Session Shaping on RADIUS

Example

To use RADIUS to set the shaping rate for a subscriber session, configure the following Cisco VSA in the user profile on RADIUS:

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default), shape(rate))"
```

When the ISG receives a RADIUS Access-Accept or change of authentication (CoA) message with this VSA included, the ISG copies the currently configured policy map applied on the session and

changes the shaping rate of the transient parent class-default class to the shaping rate specified in the VSA. The ISG makes changes only to the transient policy; no changes are made to the original policy map. After changing the transient policy, the ISG applies the transient policy to the subscriber session.

Configuring per-Service Shaping and Policing

Configuring a Hierarchical QoS Child Policy with Shaping and Policing on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]
6. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a policy map and enters policy-map configuration mode.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class voip`	Configures QoS parameters for the traffic class you specify and enters policy-map class configuration mode. • *class-name* —Name of a traffic class you previously configured using the **class-map** command.

	Command or Action	Purpose
Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.
Step 6	**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 10000`	Configures traffic policing. **Note** Specify either the **shape** command or the **police** command for a traffic class, but not both commands for the same class.
Step 7	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to Privileged EXEC mode. **Note** Repeat steps 3 through 7 for each child policy map you want to create, or repeat steps 4 through 7 for each traffic class you want to define in each policy map.

Configuring a Hierarchical QoS Parent Policy with Shaping and Policing on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*]
6. **service-policy** *policy-map-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map parent`	Creates or modifies a policy map.
Step 4	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Modifies the class-default traffic class and enters policy-map class configuration mode.
Step 5	**shape average** *mean-rate* [*burst-size*] [*excess-burst-size*] [**account** {**qinq** | **dot1q** | **user-defined** *offset* } **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate.
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the child policy map to the parent class-default class. • *policy-map-name* —Name of the child policy map.
Step 7	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

Configuring per-Service Shaping and Policing on RADIUS

To use RADIUS to set the shaping and policing rate for a subscriber service, configure the following Cisco VSAs in the service profile on RADIUS:

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), shape(rate))"
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), police(rate))"
```

When the ISG receives a RADIUS Access-Accept or CoA message with these VSAs included, the ISG copies the originally configured policy map that is active on the session and changes the shaping or policing rate of the traffic class specified in the class-list field. The ISG makes changes only to the transient policy and applies the transient policy to the subscriber service; no changes are made to the original policy map.

Note Per-service shaping and policing do not apply to the parent class-default class.

For more information, see the “RADIUS Attributes” section.

Verifying RADIUS-Based Policing

To verify the configuration of RADIUS-based policing on the ISG, use any of the following commands in privileged EXEC mode.

Command	Purpose
show policy-map interface	Displays the configuration of all classes configured for all policy maps attached to all interfaces.
show policy-map interface *interface* [*input* | *output]*]	Displays the configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. • *interface* is the name of the interface or subinterface. • **input** indicates the statistics for the attached inbound policy. • **output** indicates the statistics for the attached outbound policy. If you do not specify **input** or **output**, the router shows information about all classes that are configured for all inbound and outbound policies attached to the interface you specify.
show policy-map *policy-map-name*	Displays the configuration of all of the traffic classes contained in the policy map you specify. • *policy-map-name* is the name of the policy map for the configuration information you want to appear. • If you do not specify a value for the *policy-map-name*argument, the command shows the configuration of all policy maps configured on the router.
show policy-map *policy-map-name* **class** *class-name*	Displays the configuration of the class you specify. The policy map you specify includes this class. • *policy-map-name* is the name of the policy map that contains the class configuration you want to appear. • *class-name* is the name of the class whose configuration you want to. If you do not specify a value for the *class-name*argument, the command shows the configuration of all of the classes configured in the policy map.
show policy-map session [**output** | **output** | *uid*]	Displays the inbound or outbound policy maps configured per session. Also displays the dynamic policy map that is applied to the subscriber session. If you do not specify any arguments, the command shows all sessions with configured policy maps, which might impact performance. • **input** indicates inbound policy maps. • **output** indicates outbound policy maps. • *uid* is the session ID.
show running-config	Displays the running-configuration file, which contains the current configuration of the router, including the default QoS policy.

Command	Purpose
show running-config interface *interface*	Displays the configuration of the interface you specify that is currently configured in the running-config file, including any service policies attached to the interface.

Configuration Examples for RADIUS-Based Policing

Example: Adding Parameterization of QoS ACLs

The following example shows how to parameterize the set source IP address and destination IP address parameter, set-src-dst-ip-in-acl, through CoA or Access-Accept messages. The QoS parameterized service is added in the parameterized QoS service RADIUS form:

```
VSA252 0b q-p-out=IPOne(1)((c-d,voip)13(10.10.1.0/28,10.3.20/29))
! The above command activates the service in a CoA message.
vsa cisco generic 1 string
"qos-policy-out=add-class(sub,(class-default,voip),set-src-dst-ip-in-acl(10.10.1.0/28,10.3.20/29))"
! The above command activates the service in a Access-Accept message.
```

The router is configured as follows:

```
ip access-list extended IPOne-acl
 remark Voice-GW
 permit ip host 10.0.1.40 any
!
class-map match-any voip
  match access-group name IPOne-acl
!
class-map type traffic match-any IPOne
 match access-group output name IPOne-acl
 match access-group input name IPOne-acl
 !
!
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
!
policy-map output_parent
  class class-default
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action drop

  service-policy output_child
  !
!
policy-map output_child
  class voip
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action drop

    !
  !
!
! RADIUS relays the string for service activation. After the VSA is received, a new ACL is
 created.
ip access-list extended IPOne-acl-10.10.1.0/28,10.3.20/29
```

```
 remark Voice-GW
 permit ip host 10.0.1.40 any
 permit ip 10.10.1.0 0.0.0.15 any
 permit ip any 10.10.1.0 0.0.0.15
 permit ip 10.3.2.0 0.0.0.7 any
 permit ip any 10.3.2.0 0.0.0.7
!
! A new class map is created.
class-map match-any voip-10.10.1.0/28,10.3.20/29
  match access-group name IPOne-acl-10.10.1.0/28,10.3.20/29
!
! The old class is replaced with the new class in the output QoS policy of the subscriber,
 along with any other attributes.
```

Adding Parameterization of QoS ACLs with ISG Service Accounting

The following example shows how to add QoS accounting by configuring the ISG accounting service:

```
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
 class type traffic default in-out
 !
!
! After the VSA is received, a new traffic class map is created on the service.
class-map type traffic match-any IPOne-10.10.1.0/28,10.3.2.0/29
 match access-group output name IPOne-acl-10.10.1.0/28$10.3.2.0/29
 match access-group input name IPOne-acl-10.10.1.0/28$10.3.2.0/29
!
! A new ISG service is created.
policy-map type service IPOne(tc_in=IPOne-acl-10.10.1.0/28$10.3.2.0/29)
 10 class type traffic IPOne-10.10.1.0/28,10.3.2.0/29
  accounting aaa list default
 !
 class type traffic default in-out
!
```

Example: Setting the Shaping Rate Using an Access-Accept Message

The examples in this section illustrate how to set the shaping rate of a session using an access-accept message.

ISG Original Policy

This configuration example uses a RADIUS Access-Accept message to change the shaping rate of a session:

```
class-map match-any Premium
  match access-group name Premium_Dest
!
policy-map Child
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
```

```
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA adds the class-default class to the QoS policy attached to the subscriber session for outbound traffic and shapes the class-default class to 120,000 bps.

```
radius subscriber 6
  framed protocol ppp
  service framed
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default), shape(120000))"
  [New shaping rate]
```

RADIUS Access-Accept Message

The ISG receives the following RADIUS Access-Accept message. Notice that the above Cisco VSA configured in the user's profile is present in the Access-Accept message and that the parent shaping rate has changed to 120,000.

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default),
shape(120000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent. While the parent shaping rate, as previously shown, changes to 120,000, the shaping rate displayed in the transient New_Parent policy is the old rate of 10,000, as seen in the following example. The child policy remains unchanged.

```
policy-map New_Parent [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy Child
```

Example: Setting the Shaping Rate Using a CoA Message

The examples in this section illustrate how to set the shaping rate of a session using a CoA message.

ISG Original Policy

This configuration example uses a RADIUS CoA message to change the shaping rate of a session:

```
class-map match-any Premium
  match access-group name Premium_Dest
```

```
!
policy-map Child
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA adds the class-default class to the QoS policy attached to the subscriber session for outbound traffic and shapes the class-default class to 120,000 bps.

```
radius subscriber 1047
  vsa cisco 250 S192.168.1.2
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default), shape(120000))"
  [New shaping rate]
```

RADIUS CoA Message

The ISG receives the following RADIUS CoA message. Notice that the Cisco VSA configured in the user's profile above is present in the CoA message.

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.2"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default),
shape(120000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.2
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default),
shape(120000))
1d21h:
ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.2"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the CoA message, the ISG changes the shaping rate of the parent class-default class to 120,000 bps. However, the shaping rate displayed in the transient New_Parent policy is the old rate of 10,000, as seen in the following example. The child policy remains unchanged.

```
policy-map Child
  class Premium
    shape average 5000

policy-map New_Parent [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy Child
```

Example: Setting the Policing Rate Using an Access-Accept Message

The examples in this section illustrate how to set the policing rate of a traffic class using an access-accept message.

ISG Original Policy

This configuration example uses a RADIUS Access-Accept message to change the policing rate of a traffic class at the child level of a hierarchical policy:

```
class-map match-any Premium
match access-group name Premium_Dest
!
policy-map Child
  class Premium
    shape average 5000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA changes the policing rate of the Premium class in the Child policy. The Child policy is applied to the class-default class of the Parent policy.

```
radius subscriber 6
  framed protocol ppp
  service framed
  vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
```

RADIUS Access-Accept Message

The ISG receives the following RADIUS Access-Accept message. Notice that the above Cisco VSA configured in the user's profile is present in the Access-Accept message.

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
```

```
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
 police(200000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG Transient Policy

The ISG copies the service policy that is currently applied to the session and creates a transient policy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the Access-Accept message, the ISG adds the policing rate to the Premium traffic class. The Premium class is configured in the transient New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child [New cloned child policy]
  class Premium
    police 200000 [New policing rate]
    shape average 5000
!
policy-map New_Parent [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy New_Child [New cloned child policy attached to the new
 cloned parent policy]
```

Example: Setting the Policing Rate Using a CoA Message

The examples in this section illustrate how to set the policing rate of a service using a CoA message.

ISG Original Policy

This configuration example uses a RADIUS CoA message to change the policing rate of a service and is based on the following ISG configuration:

```
policy-map Child
  class Premium
    police 12000
!
policy-map Parent
  class class-default
    shape average 10000
    service-policy Child
```

RADIUS Configuration

The following Cisco VSA is configured in a user's profile on RADIUS. This VSA modifies the Premium class of the Child policy, which is applied to the class-default class of the Parent policy.

```
radius subscriber 1048
vsa cisco 250 S192.168.1.10
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
```

RADIUS CoA Message

The ISG receives the following RADIUS CoA message. Notice that the Cisco VSA configured in the user profile above is present in the CoA message.

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
 police(200000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.10
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default, Premium),
police(200000))
1d21h:
ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the Access-Accept message, the ISG changes the policing rate of the Premium traffic class from 5000 bps to 200,000 bps. The Premium class is configured in the New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child [New cloned child policy]
  class Premium
    police 200000 [New policing rate]
!
policy-map New_Parent [New cloned parent policy]
  class class-default
    shape average 10000
    service-policy New_Child [New cloned child policy attached to the new
 cloned parent policy]
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
HA commands	Cisco IOS High Availability Command Reference

Related Topic	Document Title
HA configuration	*Cisco IOS High Availability Configuration Guide*
QoS Policy Configuration	*Cisco IOS QoS: Policing and Shaping Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RADIUS-Based Policing

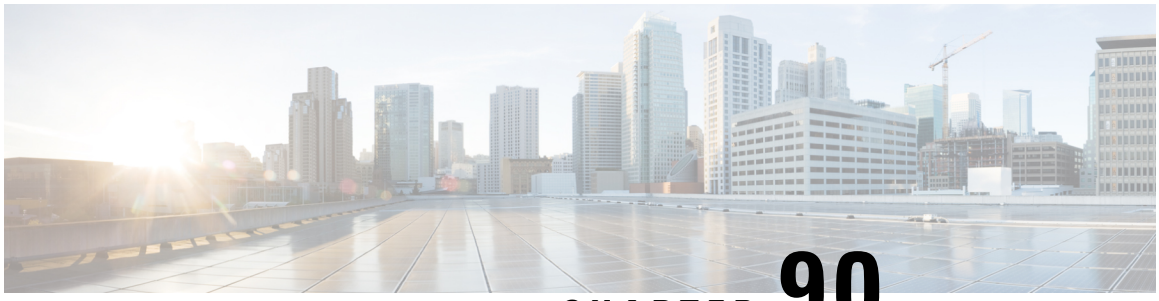
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 121: Feature Information for RADIUS-Based Policing

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: RADIUS-Based Policing	Cisco IOS XE Release 2.4	The RADIUS-Based Policing feature extends ISG functionality to allow the use of a RADIUS server to provide subscriber policy information. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.
RADIUS-Based Policing Attribute Modifications	Cisco IOS XE Release 2.4	The RADIUS-Based Policing Attribute Modifications feature allows the RADIUS server to communicate with the ISG by embedding specific attributes in Access-Accept and CoA messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services, and to modify the active QoS policy applied to a session. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.

Feature Name	Releases	Feature Information
Parameterization of QoS ACLs	Cisco IOS XE Release 2.4	The Parameterization of QoS ACLs feature provides enhancements for QoS ACLs. This feature allows the AAA device to change parameters dynamically. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router.
ISG Policy HA and RaBaPol HA	Cisco IOS XE Release 3.5S	Adds SSO and ISSU support to ISG RADIUS-based policing.



CHAPTER 90

Overview for Framed Route

Framed Route allows you to route customer additional networks (behind CPE) through customer broadband connection in ISG. Framed Route has relevance only when CPE acts as routed CPE and NAT is disabled. The broadband IPoE/PPPoE connection for CPE is created at ISG and the network behind CPE must be routed through CPE IPoE/PPPoE session in ISG. A per-user static route is downloaded to IPoE/PPP users through the Framed-Route RADIUS attribute during login.

Benefits of using Framed Route

Framed Route allows a large number of customer networks to reach via framed routes through a single ISG session.

Framed Route is supported on both IPoE and PPPoE sessions.

There is no limit enforced to the number of framed routes per session.

You don't have to configure or enable Framed Route through command line interface as it is downloaded from RADIUS.

Restrictions for Framed Route

General Restriction

Framed Route cannot be applied through a RADIUS COA.

IPoE Specific Restrictions

No support for routed session.

Dual stack is not supported.

ISG does not expect next hop information in Framed-Route AVP. ISG will replace Next hop information with CPE IP.

If CPE already has an IP address assigned, then RADIUS server should always provide CPE IP in Framed-IP-Address AVP in Access-Accept.

Configuring Framed Route

There is no manual configuration required to enable Framed Route through command line interface as it is downloaded from RADIUS.

Following are samples of the framed route configuration from RADIUS:

Framed-route configuration A

```
Cleartext-Password := "cisco”
         Service-Type = Framed-User,
         Framed-IP-Address = 40.0.0.1,
         Framed-Route += "131.1.1.0 255.255.255.0",
         Cisco-AVPair += "subscriber:accounting-list=List1“
```

Framed-route configuration B

```
Cleartext-Password := "cisco“
         Service-Type = Framed-User,
         Framed-Route = "131.1.2.0 255.255.255.0",
         Framed-Route += „131.1.3.0/24“,

         Cisco-AVPair += "subscriber:accounting-list=List2“
```

Verifying Framed Route

Use the **show subscriber session** command to verify the subscriber session output when Framed Route is installed:

```
Device# show subscriber session 1 detailed
Type: DHCPv4, UID: 1, State: authen, Identity: 000a.000b.000c
IPv4 Address: 10.0.0.1
Session Up-time: 21:31:36, Last Changed: 21:31:38
Switch-ID: 4098

Features:
Static Routes:
Class-id  Configuration Status           Source
0          This feature is enabled       Peruser
```

Use the **show ip static route** command to verify the static route configuration when Framed Route is installed:

```
Device# show ip static route
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       D1 - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng, LI - LIIN
       IR - ICMP Redirect
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - permanent
```

```
Static local RIB for default
50.0.0.0/24 is subnetted, 1 subnets
        50.0.1.0[1/0] via 10.0.0.1
60.0.0.0/24 is subsetted, 1 subnets
        60.0.1.0[1/0] via 20.0.0.1
```

Troubleshooting Framed Route

Use the following debug commands if you have any configuration issues:

- **debug subscriber feature name static-routes**{**error** | **event**}- Enables debugging of the static-route feature.
- **debug subscriber**{**error** | **event** | **feature**}- Enables debugging of subscriber sessions.
- **debug ip subscriber all**- Enables debugging of IP subscribers.
- **debug ppoe**{**errors** | **events**}- Enables debugging of PPPoE subscribers.

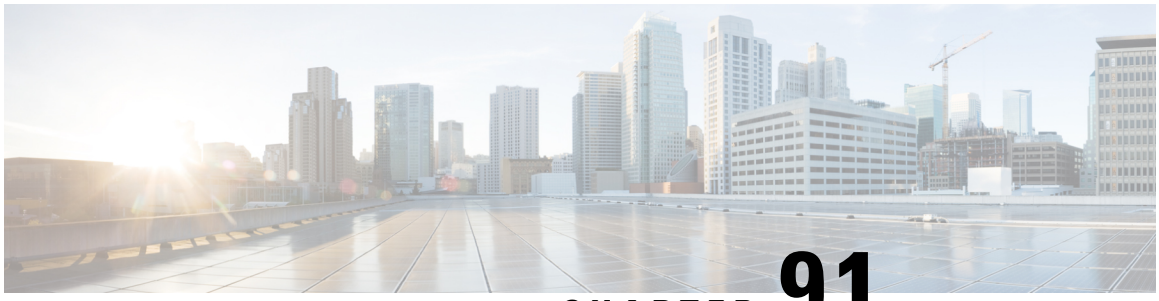
Feature Information for Framed Route

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 122: Feature Information for Framed Route

Feature Name	Releases	Feature Configuration Information
IPoE with Framed Route	Cisco IOS XE Everest 16.4.1	Framed Route allows to route customer additional networks (behind CPE) through customer broadband connection in ISG. IPoE with Framed Route has relevance only when CPE acts as routed CPE and NAT is disabled. The following commands were modified: **show ip static route**,**show subscriber session**.



CHAPTER 91

ISG Dynamic VLAN Interface Provisioning

The ISG Dynamic VLAN Interface Provisioning feature enables the automatic creation of VLAN interfaces based on the VLAN packet trigger. The VLAN interface configuration is downloaded from the RADIUS server. This module describes how to enable ISG to dynamically configure VLAN interfaces for simple IP sessions.

Prerequisites for ISG Dynamic VLAN Interface Provisioning

- Disable VLAN filtering on the corresponding SPAs by using the **hw-module subslot** *[m/n]* **ethernet vlan unlimited** command.

Note Although disabling this command avoids dropping of unknown VLAN tags, it affects other features that use VLAN filtering. For example, some QoS features like dot1p do not work when this command is disabled.

Restrictions for ISG Dynamic VLAN Interface Provisioning

- After provisioning a DVLAN interface, it is not advised to write memory as this will disable removal of the DVLAN interface.
- It is not advised to manually delete a dynamically provisioned interface. This should be done only with CoA or by using the **clear vlan-autoconfig** *interface* command.

Note You can delete up to a maximum of 200 interfaces using the **clear vlan-autoconfig** *interface* command.

- Semantic errors encountered during shell-map execution are not handled.
- You can only configure upto 64000 VLANs per system in the Cisco ASR 1000 Series Aggregation Services Routers. The following table lists the VLAN scale restrictions for the Cisco ASR 1000 Series Aggregation Services Routers RP2 and ESP40 platform with 8GB memory.

Platform Scalability	**ASR 1000 RP2+ESP40** **8GB RP2**
Number of VLANs per port	4000
Number of VLANs per SPA	8000 32000 with VLAN unlimited
Number of VLANs per system	64000
Number of QinQ VLANs per port	4000
Number of QinQ VLANs per SPA	8000 32000 with VLAN unlimited
Number of QinQ VLANs per system	64000

Information About ISG Dynamic VLAN Interface Provisioning

Overview of ISG Dynamic VLAN Interface Provisioning

This feature simplifies the VLAN sub-interface configuration by downloading the configuration details from a RADIUS-based server. These details are based on the VLAN tag of the first packet coming on the access interface. Any FSOL with a VLAN tag can bring up the dynamic VLAN interface. The configuration that is downloaded is defined in the shell map and the shell map parameters are passed through RADIUS during *Access Accept*. To de-provision the interface, you need to do it manually through CoA only.

Benefits of ISG Dynamic VLAN Provisioning

Some benefits of automatically dynamic VLAN provisioning on the Cisco ISG interface are listed below:

- You need not manually configure the VLAN sub-Interfaces on the device.
- Dynamic VLAN provisioning reduces maintenance time due to simplified operations.
- Performance is improved as the VLAN interface configurations are not included in the startup configuration.

IOS Shell Maps and Usage

The VLAN interface configuration for different VLANs is similar except that for the set of interface-specific parameters that need to be configured. These interface-specific parameters are downloaded from the RADIUS server.

The interface configuration commands are merged together in the IOS shell map to serve as a template. This template contains IOS CLI commands where the interface-specific parameters are replaced by shell variables. To configure a specific VLAN interface, the shell map is invoked with the appropriate parameters that replace these shell map variables.

The following steps describe how to use shell maps:

- Define the IOS shell map on the router through CLI.
- Configure this shell map name along with the VLAN interface configuration parameters on the RADIUS server for a specific VLAN ID.
- The VLAN interface configuration module downloads the specified IOS shell map along with the appropriate VLAN interface configuration parameters from the RADIUS server.
- The VLAN interface configuration module triggers the corresponding shell map with the appropriate number of parameters.
- Ensure that the number of configuration parameters for a specific VLAN matches the number of variables expected by the corresponding shell map.

  The various scenarios of parameter mismatch are listed below:

  - If the number of parameters are more, the extra parameters shall be ignored.
  - If the RADIUS server does not provide all the required parameters, a configuration error occurs.
  - If the RADIUS message carries a shell function name that does not exist on the device, a configuration error occurs.

- Configure separate IOS shell maps for each VLAN.
- Use the RADIUS CoA to change the VLAN interface configuration. Here, the CoA contains the IOS shell map name to be used along with the desired parameters.
- The IOS shell infrastructure synchronizes the active and standby IOS shell maps.

Configuration Examples for ISG Dynamic VLAN Interface Provisioning

Example: Configuring ISG Dynamic VLAN Interface Provisioning

```
sh running-config
Building configuration...

Current configuration : 5262 bytes
!
```

```
! Last configuration change at 19:15:51 IST Mon Jun 30 2014
!
version 15.5
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
no platform punt-keepalive disable-kernel-core
!
hostname UUT
!
boot-start-marker
boot system harddisk:asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20140618_050043_2.bin
boot-end-marker
!
shell map PROFILE20  {
 conf t
 interface GigabitEthernet0/0/4.$sub_if
 encapsulation dot1q $outer_vlan second-dot1q $in_vlan
 ip address $ip 255.255.255.0
 pppoe enable group global
 end
}
shell map PROFILE33  {
 conf t
 interface Port-channel30.$sub_if
 encap dot1q $outer_vlan second-dot1q $cvlan
 ip address $ip 255.255.255.0
 pppoe enable group global
 end
}
shell trigger PROFILE20 PROFILE20
shell trigger PROFILE33 PROFILE33
shell trigger rate rate
aqm-register-fnf
!
aaa new-model
!
!
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
 client 9.0.0.134 server-key coa
!
aaa session-id common
clock timezone IST 5 30
!
!
!
!
!
!
!
!
!


no ip domain lookup

!
```

```
!
!
!
!
!
!
!
!
!
vlan-autoconfig authorize list default password cisco
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
hw-module subslot 0/0 ethernet vlan unlimited
spanning-tree extend system-id
!
username lab password 0 lab
username CPE password 0 lab
!
redundancy
 mode sso
!
!
!
!
!
!
ip tftp source-interface GigabitEthernet0/0/0
ip tftp blocksize 8192
!
!
!
!
!
bba-group pppoe global
 virtual-template 1
!
!
interface Loopback1
 ip address 2.2.2.1 255.255.255.0
!
interface Port-channel30
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/4
 ip address 5.5.5.1 255.255.0.0
 negotiation auto
 vlan-autoconfig
!
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address pool pool1
 ppp authentication chap
!
ip local pool pool1 2.2.2.2 2.2.2.100
```

```
ip default-gateway 9.27.0.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 9.0.0.134 255.255.255.255 9.27.0.1
ip route 10.64.67.0 255.255.255.0 9.27.0.1
ip route 10.105.37.142 255.255.255.255 10.64.67.1
ip route 202.153.144.25 255.255.255.255 9.27.0.1
!
ip access-list extended A
 permit ip any any
!
access-list 10 permit any
!
!
!
radius-server host 9.0.0.134 key cisco
no radius-server vsa send accounting
no radius-server vsa send authentication
!
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
alias exec svs show vlan-autoconfig summary
alias exec svv show vlan-autoconfig vlan
alias exec sva show vlan-autoconfig access
alias exec stat show vlan-autoconfig statistics
alias exec punt_pol show platform software punt-policer | i Auto
alias exec punt_infra show platform software infrastructure punt | i Auto
alias exec punt_qfp show platform hardware qfp a infrastructure punt policer
alias exec cvs clear vlan-autoconfig stat
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 transport input all
!
!
!
end
```

Example: Configuring RSIM

VLAN Sub-Interface Creation from Radius

```
simulator radius server 10.0.1.2
Subscriber profiles for creating sub interfaces
user-name prefix Ethernet0/0:12 subscriber 26
user-name prefix Ethernet0/0:11 subscriber 25
```

```
user-name prefix Ethernet0/0:10 subscriber 24
Subscriber profile 24 25 26 are defined for creating virtual interface
simulator radius subscriber 24
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=10; ip=1.1.1.1)"
!
simulator radius subscriber 25
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=11;ip=2.2.2.2)"
!
simulator radius subscriber 26
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-service-info=PROFILE1(vlan=12;ip=3.3.3.3)"
!
```

VLAN Sub-Interface Deletion from Radius

```
Simulator radius subscriber 101
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=10"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
!
simulator radius subscriber 102
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=11"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
!
simulator radius subscriber 103
vsa cisco generic 1 string "vlan-auto-config=1"
vsa cisco generic 1 string "vac-subinterface-id=12"
vsa cisco generic 1 string "subscriber:command=vlan-autoconfig-delete"
attribute 87 string "Ethernet0/0"
Push the following subscriber profile from rsim as given below to delete a Sub interface
simulator radius request 1 coa 101
simulator radius request 1 coa 102
simulator radius request 1 coa 103
```

Additional References for ISG Dynamic VLAN Interface Provisioning

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

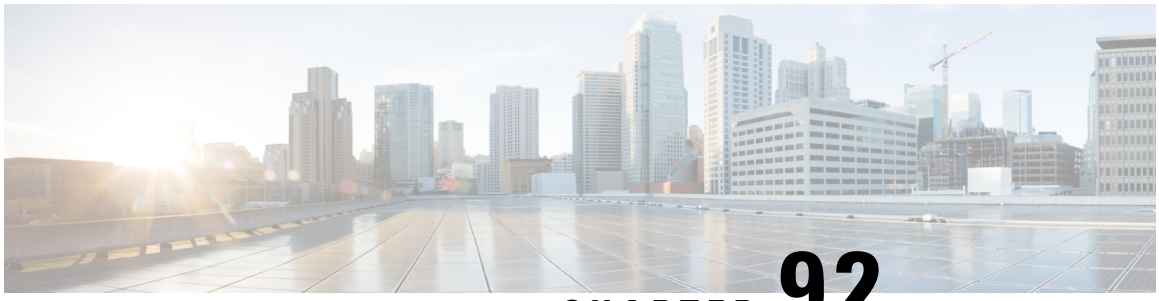
Feature Information for ISG Dynamic VLAN Interface Provisioning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 123: Feature Information for ISG Dynamic VLAN Provisioning

Feature Name	Releases	Feature Information
ISG Dynamic VLAN Provisioning		The ISG Dynamic VLAN Interface Provisioning feature enables the automatic creation of VLAN interfaces based on the VLAN packet trigger. The VLAN interface configuration is downloaded from the RADIUS server. The following command was introduced: **vlan-autoconfig**.



CHAPTER 92

Ambiguous VLAN Support for IP sessions over ISG

The Ambiguous VLAN Support for IP Sessions over ISG feature allows network service providers to define a range or ranges of inner VLANs and create queue-in-queue (QinQ) VLANs on demand. This is done by specifying a range for the inner VLAN tag in the IEEE 802.1Q-in-Q while maintaining a single outer VLAN tag for each subinterface. This module explains the Ambiguous VLAN Support for IP Sessions over ISG feature and how to configure it.

Restrictions for Ambiguous VLAN Support for IP Sessions over ISG

- Ambiguous VLANs are currently supported only for Inteliigent Services Gateway (ISG) sessions.
- IP sessions and PPP sessions are not supported on the same ambiguous subinterfaces. Hence, different ranges need to be specified for the outer VLAN tags for both IP sessions and PPP sessions.
- Only a limited feature set will be applied to each queue-in-queue (QinQ) pair as no subinterfaces are created for each QinQ pair. The available features include those applicable to the ISG session and those applicable to the ambiguous VLAN interface.
- This feature is restricted to Layer 2 unclassified MAC and DHCP-initiated ISG sessions.
- IPv6 sessions are not supported.
- This feature supports only Ethertype 0x8100. Other Ethertypes such as 0x88A8, 0x9100 and 0x9200 are not supported.
- This feature does not support Virtual Routing and Forwarding (VRF).

Information About Configuring Ambiguous VLAN Support for IP Sessions over ISG

Benefits of Ambiguous VLAN Support for IP Sessions over ISG

Ambiguous VLAN implementation for IP sessions in Intelligent Services Gateway (ISG) has the following benefits:

- The service provider only needs to know the end-user VLAN ranges instead of the individual end-user VLAN IDs.
- The ambiguous VLAN feature allows the configuration of multiple VLANs under one subinterface which leads to better Interface Descriptor Block (IDB) utilization.

Configuring Ambiguous VLAN Support for IP Sessions over ISG

You can define a range of inner VLANS and create QinQ VLANS, or you can use the keyword **any** for the system to assign any inner VLAN ID that has not been used elsewhere.

To configure a range of inner VLANS:

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000
```

or

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q 1000-2000
```

To configure the sub-interface for ambiguous VLAN:

```
configure terminal
interface GigabitEthernet1/0.200
 encapsulation dot1q 200 second-dot1q any
```

Verifying Ambiguous VLAN Support for IP Sessions over ISG Configuration

Use **show subscriber session** command to verify the configuration of Ambiguous VLAN Support for IP Sessions over ISG feature.

```
Device# show subscriber session uid 6

Type: IP, UID: 6, State: unauthen, Identity: 12.12.12.2
IPv4 Address: 12.12.12.2
Session Up-time: 00:00:34, Last Changed: 00:00:34
```

```
Switch-ID: 8221

Policy information:
  Authentication status: unauthen

Classifiers:
Class-id    Dir   Packets    Bytes                 Pri.  Definition
0           In    4          488                   0     Match Any
1           Out   4          488                   0     Match Any

Configuration Sources:
Type  Active Time  AAA Service ID  Name
INT   00:00:34     -               GigabitEthernet0/1/3.1
```

Additional References for Ambiguous VLAN Support for IP Sessions over ISG

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/c/en/us/support/index.html

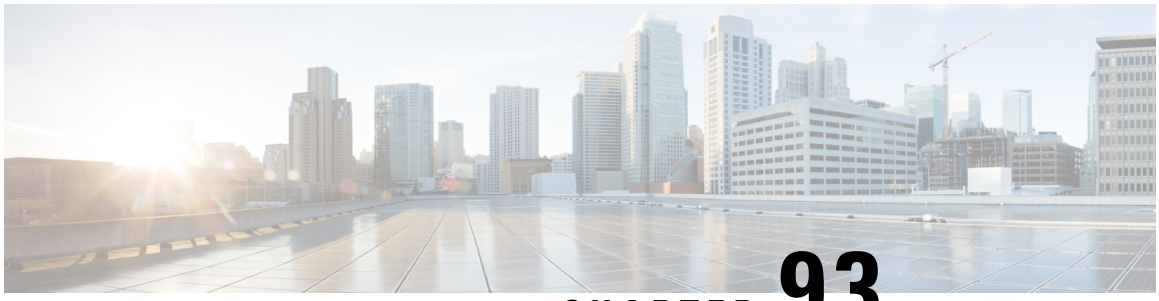
Feature Information for Ambiguous VLAN Support for IP Sessions over ISG

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 124: Feature Information for Ambiguous VLAN Support for IP Sessions over ISG

Feature Name	Releases	Feature Information
Ambiguous VLAN Support for IP Sessions over ISG	Cisco IOS XE Release 3.8S	The Ambiguous VLAN Support for IP Sessions over ISG feature allows network service providers to define a range or ranges of inner VLANs and create queue-in-queue (QinQ) VLANs on demand. This is done by specifying a range for the inner VLAN tag in the IEEE 802.1Q-in-Q while maintaining a single outer VLAN tag for each subinterface. This module explains the Ambiguous VLAN Support for IP Sessions over ISG feature and how to configure it. The following commands were introduced or modified by this feature: **encapsulation dot1q**.



CHAPTER 93

Configuring ISG Policies for Automatic Subscriber Logon

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module contains information on how to configure ISG to use specified identifiers in place of the username in authorization requests, enabling a user profile to be downloaded from an authentication, authorization, and accounting (AAA) server as soon as packets are received from a subscriber.

Prerequisites for ISG Automatic Subscriber Logon

Depending on your AAA implementation, you may need to configure one of the following identifiers in the password field of the user profile: source IP address, MAC address, remote ID, circuit ID. You may also need to configure a global address in the password field.

To use circuit ID and remote ID for authorization for IP sessions, the DSLAM must insert the circuit ID and remote ID in the DHCP Option 82 information.

To use remote ID for authorization of PPPoE sessions, the PPPoE client must provide the remote ID information in the PPPoE Tag ID or line ID.

Restrictions for ISG Automatic Subscriber Logon

The username field in an authorization request has a limit of 253 characters.

Information About ISG Automatic Subscriber Logon

Overview of ISG Automatic Subscriber Logon

Service providers commonly implement a policy at the start of IP sessions that redirects all subscriber packets to a logon portal for authentication. Following successful authentication, per-subscriber authorization data is typically returned from a AAA server. For some deployments, usually in subscriber networks that are well protected against spoofing and denial-of-service (DoS) attacks, service providers are willing to forgo authentication and trust subscriber identity. ISG automatic subscriber logon allows service providers to grant certain subscribers access to services without requiring the subscribers to log on.

ISG automatic subscriber logon enables a specified identifier to be used in place of the username in authorization requests. Enabling the AAA server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

The event that triggers automatic subscriber logon is session-start. For IP sessions, session-start occurs when a DHCP DISCOVER request is received or when an unrecognized source IP address is detected. For PPPoE sessions, session-start occurs when a client attempts to initiate a session by sending a PPPoE Active Discovery Initiation (PADI) packet.

Supported Identifiers for ISG Automatic Subscriber Logon

For IP sessions, an ISG device can be configured to use the following identifiers in place of the username in authorization requests: IP address, MAC address, circuit ID, remote ID, or a combination of the circuit ID and remote ID.

For PPPoE sessions, an ISG device can be configured to use the remote ID in place of the username in authorization requests.

Authorization Based on Circuit ID and Remote ID

The circuit ID and remote ID fields are part of the DHCP relay agent information option (also referred to as Option 82) and the PPPoE Tag VSA. These fields are inserted into DHCP and PPPoE messages by a DSLAM. An ISG device can be configured to use the circuit ID, remote ID, or a combination of circuit ID and remote ID as the username in authorization requests.

By default, the ISG device will use the circuit ID and remote ID that are provided by the Layer 2 edge access device for authorization. If the **ip dhcp relay information option** command is configured, the ISG device will use the circuit ID and remote ID that are received in a DHCP message.

Accounting Behavior When ISG Automatic Subscriber Logon Is Configured

Accounting Behavior for MAC-Address-Based Authorization

If the MAC address is sent as the username in authorization requests, the MAC address will also be sent as the Calling Station ID in accounting records.

Accounting Behavior for Remote-ID- and Circuit-ID-Based Authorization

For IP sessions that use DHCP Option 82 authorization, accounting messages are sent to the AAA server with the Circuit ID and Remote ID Cisco VSAs. Although you can configure a combination of circuit ID and remote ID as the username for authorization, the attributes are sent individually in accounting records. You can also configure the circuit ID and remote ID to be sent together in accounting records as the NAS Port ID.

For PPPoE sessions, the Remote ID VSA is sent in accounting records, and the remote ID is also sent as the NAS Port ID.

If the **radius-server attribute 31 remote-id** command is configured, the remote ID is sent in accounting records as the Calling Station ID.

How to Configure ISG Policies for Automatic Subscriber Logon

Identifying Traffic for Automatic Logon in a Control Policy Class Map

Perform this task to configure a control policy class map that specifies the traffic to which ISG automatic subscriber logon will apply.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type control match-all** *class-map-name*
4. Do one of the following:
   - **match source-ip-address** *ip-address subnet-mask*
   -
   - **match nas-port circuit-id** *name*
   -
   - **match nas-port remote-id** *name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**class-map type control match-all** *class-map-name* **Example:** `Router(config)# class-map type control match-all TAL-subscribers`	Creates a control class map, which defines the conditions under which the actions of a control policy map will be executed.

Step 4	Do one of the following:
	• **match source-ip-address** *ip-address subnet-mask*
	•
	• **match nas-port circuit-id** *name*
	•
	• **match nas-port remote-id** *name*
	Example:
	`Router(config-control-classmap)# match source-ip-address 10.1.1.0 255.255.255.0`
	Example:
	Example:
	`Router(config-control-classmap)# match nas-port circuit-id circuit1`
	Example:
	Example:
	`Router(config-control-classmap)# match nas-port remote-id remote1`
		Creates a condition that will evaluate true if a subscriber's source IP address matches the specified IP address.
		or
		Creates a condition that will evaluate true if a subscriber's circuit ID matches the specified value.
		or
		Creates a condition that will evaluate true if a subscriber's remote ID matches the specified value.

Step 5	**end** **Example:** `Router(config-control-classmap)# end`	(Optional) Returns to privileged EXEC mode.

Configuring an ISG Control Policy for Automatic Subscriber Logon

Perform this task to configure an ISG control policy that initiates subscriber authorization and inserts a specified identifier into the username field of the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Creates or modifies a control policy map, which is used to define a control policy.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Specifies a control class, which defines the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the task "Identifying Traffic for Automatic Logon in a Control Policy Class Map, on page 1321".
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address`	Inserts the specified identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

What to Do Next

You must apply the control policy to a context by using the **service-policy type control** command. For information about applying control policies, see the module "Configuring ISG Control Policies".

You may want to configure policies to determine what should happen for autologon subscribers whose IP address or MAC address authorization fails; for example, you may want to redirect the subscriber to the policy server for authentication.

Enabling the Remote-ID to Be Sent as the Calling-Station-ID

Perform this task to enable the ISG device to send the remote ID in the Calling-Station-ID (attribute 31) field of accounting records and access requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 31 remote-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 31 remote-id** **Example:** `Router#(config) radius-server attribute 31 remote-id`	Enables the ISG device to send the remote ID in the Calling Station ID (attribute 31) field of accounting records and access requests.

Verifying ISG Automatic Subscriber Logon

Perform this task to determine whether or not automatic subscriber logon was successful.

SUMMARY STEPS

1. **enable**
2. **show subscriber session**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Step 2 **show subscriber session**

Use the **show subscriber session** command to display information about ISG subscriber sessions. If the output shows that a session was brought up in the state "authen", automatic subscriber authorization was successful. If automatic subscriber authorization was not successful, the session will still be brought up, but in the state "unauthen".

The following sample output shows information for a session for which automatic subscriber authorization was successful:

Example:

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 3
Identifier: aabb.cc01.3000
```

SIP subscriber access type(s): IP

Example:

```
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:24, Last Changed: 00:00:21

Policy information:
  Authentication status: authen
  Rules, actions and conditions executed:
    subscriber rule-map DEFAULT
      condition always event session-start
        1 authorize identifier mac-address

Session inbound features:
 Feature: IP Idle Timeout
  Timeout value is 600
  Idle time is 00:00:21
Configuration sources associated with this session:
```

Interface: GigabtiEthernet0/0/0, Active Time = 00:00:24

Configuration Examples for ISG Automatic Subscriber Logon

Automatic Subscriber Logon Based on IP Address Example

In the following example, if the client is from the 1.1.1.0 subnet, the ISG sends an authorization request to the list "TAL_LIST" with the subscriber's source IP address as the username. If the authorization request is successful, any automatic-activation services specified in the returned user profile are activated for the session, and the execution of rules within the control policy stops. If the authorization is not successful, the rule

execution proceeds, and the subscriber is redirected to the policy server to log in. If the subscriber does not log in within five minutes, the session is disconnected.

ISG Configuration

```
subscriber service password cisco
interface GigabitEthernet0/0/0
 service-policy type control RULEA
aaa authorization network TAL_LIST group radius
aaa authentication login LOCAL local
access-list 100 permit ip any any
class-map type traffic match-any all-traffic
 match access-group input 100
 match access-group output 100
policy-map type service redirectprofile
 class type traffic all-traffic
  redirect to ip 10.0.0.148 port 8080
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDF
 match timer TIMERB
 match authen-status unauthenticated
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier source-ip-address
  2 service-policy type service aaa list LOCAL name redirectprofile
  3 set-timer TIMERB 5 minutes
!
 class type control CONDF event timed-policy-expiry
  1 service disconnect
```

User Profile Configuration

```
1.1.1.1 Password = "cisco"
 Service-Type = Outbound,
 Cisco:Account-Info = "AAuto-Internet;proxy-user;cisco"
```

Service Profile Configuration

```
Auto-Internet Password = "cisco"
 Cisco:Service-Info = "IAuto-Internet",
 Cisco-Avpair = "traffic-class=input access-group 100"
proxy-user Password = "cisco"
```

Idle-Timeout = 5

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

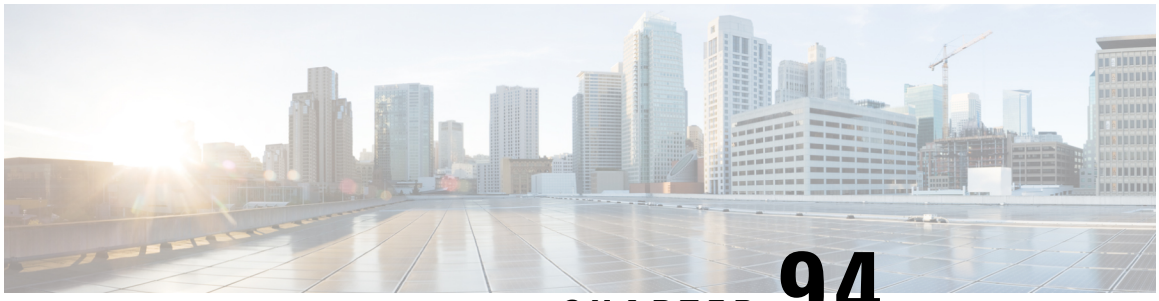
Feature Information for ISG Automatic Subscriber Logon

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 125: Feature Information for ISG Automatic Subscriber Logon

Feature Name	Releases	Feature Configuration Information
ISG: Session: Authentication (MAC, IP)	Cisco IOS XE Release 2.2	ISG automatic subscriber logon enables an IP address or MAC address to be used in place of the username in authorization requests. This functionality allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.
ISG: Authentication: DHCP Option 82 Line ID - AAA Authorization Support	Cisco IOS XE Release 2.2	This feature enhances ISG automatic subscriber logon by providing support for authorization on the basis of the circuit-id and remote-id.



CHAPTER 94

Configuring DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. The DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon feature enables service providers to provision triple-play services to households by supporting transparent automatic logon (TAL) through Dynamic Host Configuration Protocol (DHCP) option 60 and option 82, and wholesale IP sessions through the virtual private network (VPN) ID extension to option 82.

Prerequisites for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

For vendor-class ID (option 60) to be used for authorization, the vendor-class ID must be inserted by the customer appliance (that is, the PC, phone, or set-top box) in the DHCP option 60 information.

For provisioning of wholesale IP sessions, the VPN-ID must be inserted in the DHCP option 82 information along with the circuit ID and the remote ID.

Restrictions for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

RADIUS proxy users are not supported by this feature.

Information About DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

ISA Automatic Subscriber Logon

TAL enables a specified identifier to be used in place of the username in authorization requests. Enabling the Authentication, Authorization, and Accounting (AAA) server to authorize subscribers on the basis of a specified identifier allows subscriber profiles to be downloaded from the AAA server as soon as packets are received from subscribers.

Session start is the event that triggers TAL. For DHCP-initiated IP sessions, session start occurs when a DHCP DISCOVER request is received.

Authorization Based on Option 60 and Option 82

The circuit ID and remote ID fields (option 82) are part of the DHCP relay agent information option. A digital subscriber line access multiplexer (DSLAM) inserts the option 82 fields into DHCP messages; the customer appliance inserts the option 60 fields.

You can configure an ISG policy to use the circuit ID, remote ID, or vendor class ID, or a combination of the three, as the username in authorization requests. Alternatively, you can configure an ISG policy to use the NAS-Port-ID as the identifier for authorization. When you use the NAS-Port-ID as the identifier, you can configure it to include a combination of circuit ID, remote ID, and vendor-class ID.

By default, the ISG uses the circuit ID and remote ID that are provided by the Layer 2 edge-access device for authorization. The configuration of the **ip dhcp relay information option** command determines whether the ISG uses the option 82 information received, generates its own, or (when the **encapsulate** keyword is specified) encapsulates a prior option 82 along with its own option 82. For more information, see the "Configuring the Cisco IOS DHCP Relay Agent" section of the *Cisco IOS IP Addressing Services Configuration Guide* .

If the NAS-Port-ID is not configured to include option 60 and option 82, the NAS-Port-ID is populated with the ISG interface that received the DHCP relay agent information packet; for example, Ethernet1/0.

DHCP Option 82 with VPN-ID Suboption

To support wholesale services for IP sessions, the VPN-ID, together with the circuit ID and remote ID, must be specified in authorization requests. The DHCP option 60 and option 82 with VPN-ID Support for Transparent Automatic Logon feature enables you to include two sets of option 82 information in a single message so that devices within a household can be differentiated:

- The first set of option 82 information carries household information and option 60 to associate the device within the household.
- The second set of option 82 information, if VPN-ID is configured, carries the VPN information for the household.

The DHCP server processes the option 82 information, forwarded by the relay, with the VPN-ID, remote ID, circuit ID, and option 60 information to allocate an address.

How to Configure DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

You can configure an ISG policy for TAL using either a username or the NAS-Port-ID for authorization.

Configuring an ISG Control Policy Using Option 60 and Option 82

Perform this task to configure an ISG control policy that inserts a specified identifier into the username field of the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:**	Enters control policy-map configuration mode to define a control policy.

	Command or Action	Purpose
	`Router(config)# policy-map type control TAL`	
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier** *identifier-type* [**plus** *identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier source-ip-address vendor-class-id plus circuit-id plus remote-id`	Inserts the specified identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring an ISG Control Policy Using NAS-Port-ID

Perform this task to configure an ISG control policy that uses NAS-Port-ID in the authorization request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control TAL`	Enters control policy-map configuration mode to define a control policy.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control TAL-subscribers event session-start`	Enters control policy-map class configuration mode to define the conditions that must be met in order for an associated set of actions to be executed. • Specify the control class-map that was configured in the section "Identifying Traffic for Automatic Logon in a Control Policy Class Map".
Step 5	*action-number* **authorize** [**aaa** {*list-name* | **list** {*list-name* | **default**}} [**password** *password*]] [**upon network-service-found** {**continue** | **stop**}] [**use method** *authorization-type*] **identifier nas-port** **Example:** `Router(config-control-policymap-class-control)# 1 authorize aaa list TAL_LIST password cisco identifier nas-port`	Inserts the NAS port identifier into the username field of authorization requests.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NAS-Port-ID to Include Option 60 and Option 82

Perform this task to include option 60 and option 82 in the NAS-Port-ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute nas-port-id include** {*identifier1* [**plus** *identifier2*] [**plus** *identifier3*]} [**separator** *separator*] **Example:** `Router(config)# radius-server attribute nas-port-id include circuit-id plus vendor-class-id`	Includes DHCP relay agent information option 60 and option 82 in the NAS-Port-ID.

Configuration Examples for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

Example Option 60 and Option 82 in NAS-Port-ID

The following example uses the **radius-server attribute nas-port-id include** command to configure option 60 and option 82 authorization using circuit ID, remote ID, and vendor-class ID:

```
interface Ethernet0/0
 service-policy type control RULEA
!
interface Ethernet1/0
 service-policy type control RULEB
!
class-map type control match-all CONDA
 match source-ip-address 10.1.1.0 255.255.255.0
!
class-map type control match-all CONDB
 match vendor-class-id vendor1
!
policy-map type control RULEA
 class type control CONDA event session-start
  1 authorize aaa list TAL_LIST password cisco identifier vendor-class-id
!
policy-map type control RULEB
 class type control CONDB event session-start
  1 authorize aaa list TAL_LIST password cisco identifier nas-port
!
radius-server attribute nas-port-id include circuit-id plus remote-id plus vendor-class-id
 separator #
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Configuring ISG policies for automatic subscriber logon	"Configuring ISG Policies for Automatic Subscriber Logon" module in the *Intelligent Services Gateway Configuration Guide*
Configuring a DHCP relay agent	"Configuring the Cisco IOS DHCP Relay Agent" module in the *IP Addressing Services Configuration Guide*

Standards

Standard	Title
None	-

MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	-

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

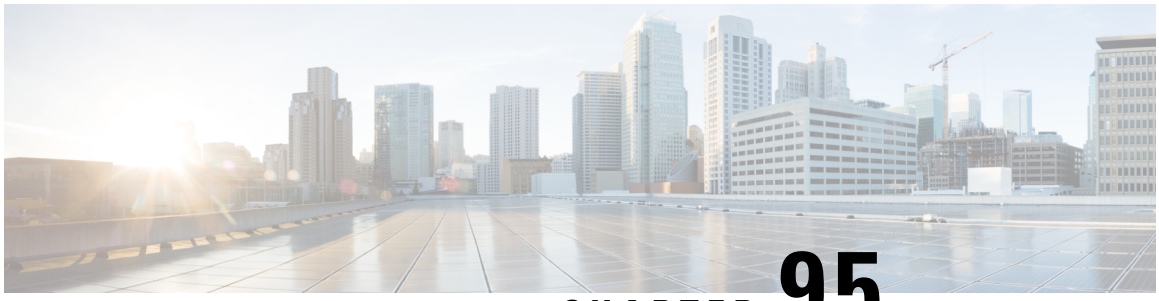
Feature Information for DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 126: Feature Information for DHCP Option 60 and Option 82 Support and VPN-ID Support

Feature Name	Releases	Feature Information
ISG: Authentication: DHCP Option 60 and Option 82 with VPN-ID Support for Transparent Automatic Logon	Cisco IOS XE Release 3.1S	Enables service providers to support TAL through DHCP option 60 and option 82 and wholesale IP sessions through the VPN-ID extension to option 82. The following commands were introduced or modified: **radius-server attribute nas-port-id include**



CHAPTER 95

Enabling ISG to Interact with External Policy Servers

Intelligent Services Gateway (ISG) is a software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This document describes how to enable the ISG to retrieve session policies or accept dynamic updates to session policies from external policy servers.

Restrictions for ISG Interaction with External Policy Servers

The ISG and external policy servers should be available in the same virtual routing and forwarding (VRF) instance.

Information About ISG Interaction with External Policy Servers

Initial and Dynamic Authorization

ISG works with external devices, referred to as *policy servers* that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG and external policy servers: initial authorization and dynamic authorization.

In the initial authorization model, ISG must retrieve policies from the external policy server at specific points in a session. In this model, the external policy server is typically an authentication, authorization, and accounting (AAA) server that uses RADIUS. ISG is the RADIUS client. Instead of a AAA server, some systems use a RADIUS proxy component that converts to other database protocols, such as Lightweight Directory Access Protocol (LDAP).

The dynamic authorization model allows the external policy server to dynamically send policies to ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an

administrator, or applications can change policies on the basis of some algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduces peer-to-peer capability to RADIUS that enables ISG and the external policy server to act as the RADIUS client and server respectively.

Triple Key Authentication for ISG

Triple key authentication is a method of authenticating users based on their username, password, and location after ISG redirects them to the Cisco Service Management Engine (SME) portal. The SME server provides the location based on the source IP address of the subscriber being authenticated. Before the Triple Key Authentication Support feature was introduced, users were authenticated only on the basis of the username and password (two-key authentication). The Triple Key Authentication Support feature also eases migration from Service Selection Gateway (SSG) to an ISG platform because SSG uses triple key authentication.

For SSG, the Cisco Subscriber Edge Services Manager (SESM) server populates RADIUS attribute 31 (calling-station ID) in the user-login request that it sends to the SSG with a string containing the subscriber's location. The SSG then includes this location string in the access-request message that it sends to the RADIUS server where the login is authenticated based on the username, password, and location string.

With ISG triple key authentication, the ISG sends the location string within a Cisco vendor-specific attribute (VSA) that is included in the access-request message to the RADIUS server.

The location information is received from SME as Cisco VSA 250. This location information is included in session authentication requests, session accounting requests from the ISG, and prepaid authorization requests.

The table below shows the Cisco vendor-specific non-AVPair attribute used for triple key authentication.

Table 127: Cisco Vendor-Specific Non-AVPair Attribute

Sub-AttrID	Attribute Type	Value	Function	Example	Used in
250	account-info	L<location-string>	Third key in triple key authentication	LWiFiHotSpot001	Acc-Req CoA Req Accounting

How to Enable ISG to Interact with External Policy Servers

Configuring ISG as a AAA Client

Perform this task to configure AAA method lists and enable ISG to retrieve policies from a AAA server. This task must be performed for both initial and dynamic authorization models.

Before you begin

The servers and server groups referenced by the AAA methods must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]

4. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands level** | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
6. **aaa authorization subscriber-service** {**default** | *list-name*} *method1* [*method2...*]
7. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication login** {**default**	*list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login PPP1 group radius`	Specifies one or more AAA authentication methods to be used at login.
Step 4	**aaa authentication ppp** {**default**	*list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	**aaa authorization** {**network**	**exec**	**commands level**	**reverse-access**	**configuration**} {**default**	*list-name*} [*method1* [*method2...*]] **Example:** `Router(config)# aaa authorization network NET1 radius`	Specifies one or more AAA authorization methods to be used for restricting subscriber access to a network.
Step 6	**aaa authorization subscriber-service** {**default**	*list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authorization subscriber-service default radius`	Specifies one or more AAA authorization methods for ISG to use in providing a service.

	Command or Action	Purpose
Step 7	**aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands level**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **Example:** `Router(config)# aaa accounting network default start-stop group radius`	Enables AAA accounting of requested services for billing or security purposes.
Step 8	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Configuring ISG as a AAA Server

Dynamic authorization allows a policy server to dynamically send policies to ISG. Perform this task to configure ISG as a AAA server and enable dynamic authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**name** \| *ip-address*} [**key** [**0** \| **7**] *word*] [**vrf** *vrf-id*]
5. **port** *port-number*
6. **server-key** [**0** \| **7**] *word*
7. **auth-type** {**all** \| **any** \| **session-key**}
8. **ignore** {**server-key** \| **session-key**}
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures ISG as a AAA server and enters dynamic authorization local server configuration mode.
Step 4	**client** {**name** | *ip-address*} [**key** [**0** | **7**] *word*] [**vrf** *vrf-id*] **Example:** `Router(config-locsvr-da-radius)# client 10.76.86.90 key cisco`	Specifies a client with which ISG will be communicating.
Step 5	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1600`	Specifies the RADIUS server port. • Default is 1700.
Step 6	**server-key** [**0** | **7**] *word* **Example:** `Router(config-locsvr-da-radius)# server-key cisco`	Specifies the encryption key shared with the RADIUS client.
Step 7	**auth-type** {**all** | **any** | **session-key**} **Example:** `Router(config-locsvr-da-radius)# auth-type all`	Specifies the attributes to be used for session authorization.
Step 8	**ignore** {**server-key** | **session-key**} **Example:** `Router(config-locsvr-da-radius)# ignore session-key`	Configures ISG to ignore the shared encryption key or attribute 151.
Step 9	**end** **Example:** `Router(config-locsvr-da-radius)# end`	Exits dynamic authorization local server configuration mode.

Enabling the Location VSA for Triple Key Authentication

Perform this task to enable ISG to include the location VSA in authentication and accounting requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server vsa send accounting**

5. **radius-server vsa send authentication**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA.
Step 4	**radius-server vsa send accounting** **Example:** `Router(config)# radius-server vsa send accounting`	Enables ISG to recognize and use accounting VSAs as defined by RADIUS attribute 26.
Step 5	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Enables ISG to recognize and use authentication VSAs as defined by RADIUS attribute 26.
Step 6	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Configuration Examples for ISG Interaction with External Policy Servers

Example: Enabling ISG to Interact with External Policy Servers

The following example shows how to configure ISG as a AAA client.

```
aaa group server radius CAR_SERVER
 server 10.100.2.36 auth-port 1812 acct-port 1813

aaa authentication login default none
aaa authentication login IP_AUTHEN_LIST group CAR_SERVER
aaa authentication ppp default group CAR_SERVER
aaa authorization network default group CAR_SERVER
aaa authorization subscriber-service default local group radius
aaa accounting network default start-stop group CAR_SERVER
```

The following example shows how to configure ISG as a AAA server.

```
aaa server radius dynamic-author
  client 10.76.86.90 server-key cisco
  port 1600
  server-key cisco
  auth-type all
  ignore session-key
```

Example: Enabling the Location VSA for Triple Key Authentication

The following example shows how to enable ISG to use VSAs for accounting and authentication.

```
aaa new-model
radius-server vsa send accounting
radius-server vsa send authentication
```

The following example shows an authentication record with the session information, including the location attribute. You can display this output by using the **debug radius accounting** command or the **gw-accounting syslog** command.

```
Device# debug radius accounting

*Feb  5 01:20:50.413: RADIUS/ENCODE: Best Local IP-Address 10.0.1.1 for Radius-Server
10.0.1.2
*Feb  5 01:20:50.425: RADIUS(0000000F): Send Access-Request to 10.0.1.2:1645 id 1645/5, len
 107
*Feb  5 01:20:50.425: RADIUS:  authenticator 4D 86 12 BC BD E9 B4 9B - CB FC B8 7E 4C 8F
B6 CA
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  19
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 13  "LWiFiHotSpot001"
*Feb  5 01:20:50.425: RADIUS:  Calling-Station-Id  [31]  16  "AAAA.BBBB.CCCC"
*Feb  5 01:20:50.425: RADIUS:  User-Name           [1]   7   "george"
*Feb  5 01:20:50.425: RADIUS:  User-Password       [2]   18  *
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
*Feb  5 01:20:50.425: RADIUS:  NAS-Port            [5]   6   0
*Feb  5 01:20:50.425: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Feb  5 01:20:50.425: RADIUS:  NAS-IP-Address      [4]   6   10.0.1.1
*Feb  5 01:20:50.425: RADIUS(0000000F): Started 5 sec timeout
*Feb  5 01:20:50.425: RADIUS: Received from id 1645/5 10.0.1.2:1645, Access-Accept, len 68
*Feb  5 01:20:50.425: RADIUS:  authenticator 49 A1 2C 7F C5 E7 9D 1A - 97 B3 E3 72 F3 EA
56 56
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  17
*Feb  5 01:20:50.425: RADIUS:   ssg-account-info   [250] 11  "S10.0.0.2"
*Feb  5 01:20:50.425: RADIUS:  Vendor, Cisco       [26]  31
*Feb  5 01:20:50.425: RADIUS:   Cisco AVpair       [1]   25  "accounting-list=default"
*Feb  5 01:20:50.433: RADIUS(0000000F): Received from id 1645/5
*Feb  5 01:20:50.437: RADIUS/ENCODE(0000000F):Orig. component type = Iedge IP SIP
*Feb  5 01:20:50.437: RADIUS(0000000F): Config NAS IP: 0.0.0.0
*Feb  5 01:20:50.437: RADIUS(0000000F): sending
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	Part 1, "Authentication, Authorization, and Accounting (AAA)," *Cisco IOS XE Security Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

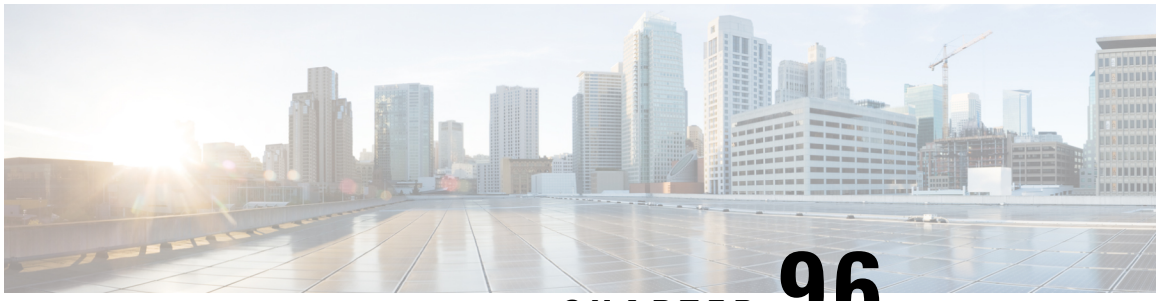
Feature Information for ISG Interaction with External Policy Servers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 128: Feature Information for ISG Interaction with External Policy Servers

Feature Name	Releases	Feature Information
ISG—Policy Control Policy Server CoA	Cisco IOS XE Release 3.3SG	This feature provides ISG support for the RADIUS Change of Authorization (CoA) extension, which facilitates dynamic authorization. This feature was integrated into Cisco IOS XE Release 3.3SG.
ISG—Session Lifecycle Packet of Disconnect (POD)	Cisco IOS XE Release 3.3SG	This feature enables an external policy server to terminate an ISG session when it receives a RADIUS Packet of Disconnect (POD).



CHAPTER 96

Configuring ISG Subscriber Services

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG defines a *service* as a collection of policies that can be applied to any subscriber session. This module describes how ISG subscriber services work, how to configure services and traffic classes that may be used to qualify policies defined within a service, and how to activate services.

Restrictions for ISG Subscriber Services

- Only one nondefault traffic class can be configured in each service.
- When multiple services are active on a given session, class-based actions are executed on a first-match basis only; in other words, once a class is matched, the actions associated with that class will be executed, and no other class will be matched.
- Removing or modifying a feature in the configuration, for example an access control list (ACL), is not supported by active sessions that reference that feature.
- If the input ACL or output ACL that is configured in a traffic class map is not defined, or if the protocol of these ACLs is not the same (IPv4 versus IPv6), the traffic class installation fails and the service is not applied. If this failure occurs at session start, the session is not established. IPv4 ACLs are defined with the **ip access-list** command; IPv6 ACLs are defined with the **ipv6 access-list** command.
- ISG supports only single-stack traffic classes; a particular traffic class can classify either IPv4 or IPv6 traffic but not both.
- If any new service needs to be defined when the sessions are active, follow the order to update the configuration:
  1. ACL definition
  2. Class-map definition

3. Policy-map service definition
4. Service name in Policy rule or update dynamically through CoA.

Information About ISG Subscriber Services

ISG Services

An ISG service is a collection of policies that may be applied to a subscriber session. ISG services can be applied to any session, regardless of subscriber access media or protocol, and a single service may be applied to multiple sessions. An ISG service is not necessarily associated with a destination zone or a particular uplink interface.

Services can be defined in two ways: in a service policy map that is configured on the ISG device by using the CLI, and in a service profile that is configured on an external device, such as an authentication, authorization, and accounting (AAA) server. Although they are configured differently, service policy maps and service profiles serve the same purpose: they contain a collection of traffic policies and other functionality that can be applied to a subscriber session. Traffic policies determine which functionality will be applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, a specific type of traffic policy that determines how session data packets will be forwarded to the network.

Primary Services

When a network-forwarding policy is included in a service profile or service policy map, the service is known as a *primary service* . Primary services are mutually exclusive and may not be simultaneously active. Upon activation of a new primary service, ISG will deactivate the existing primary service and any other services dependent on the existing primary service through association with a service group.

If a primary service is deactivated, sessions may be left without a network-forwarding policy, that is, with no means to route or forward packets. A policy may be applied to defend against this condition such that a specific service is activated upon deactivation of all others (or all other primary services). This backup service would return network-forwarding policy to the session and allow the subscriber to reach a web portal. However, it should be noted that an IP session will not be automatically terminated when all services are deactivated unless such a policy has been defined and applied.

Traffic Classes and Traffic Class Priority

ISG traffic classes provide differentiated behavior for different traffic streams to and from a particular subscriber. Each traffic stream is represented by a classification and a set of applied features. A traffic class, also known as a flow, is a kind of service.

For traffic to be classified into streams, you must specify an access control list (ACL) that classifies the traffic and the direction of the traffic to which the ACL applies (inbound or outbound). Optionally, the priority of the traffic class can also be specified. Traffic that meets the specifications of a traffic class is said to *match* the traffic class. Once a match is made, features defined in the traffic policy are executed for that traffic class.

The priority of a traffic class determines which class is used first for a specified match if more than one traffic policy has been activated for a single session. In other words, if a packet matches more than one traffic class, it is classified to the class with the higher priority.

Packets that do not match any of the ACLs are considered part of the default traffic class and are processed as if a traffic policy was not applied to the session. A default class exists for every service. The default action of the default class is to pass traffic, or the default class can be configured to drop traffic. Default traffic is accounted for in the main session accounting. A service can contain one traffic class and one default class.

ISG traffic classes are created dynamically, either at session start or later during the life of the session, when a service with a classification (the class definition of the service contains at least one named or numbered ACL) is applied to a session. A service with a classification is called a flow service. A service without a classification is called a classless service.

Traffic classes are assigned unique identifiers that can be tracked with Cisco IOS **show** commands.

Flow Classifiers

In Cisco IOS XE Release 3.3S and later releases, separate sessions are no longer created for each traffic class; the traffic class is handled as a flow within the parent subscriber session.

A flow, or traffic class, represents a subset of subscriber traffic identified by a pair of class identifiers. Each class identifier, or classifier, represents a single class or a directional flow. Traffic can have a classifier in either or both directions. If there is no classifier in a particular direction, traffic in that direction is not subjected to the flow.

The ISG classifier is responsible for managing and enforcing classifiers and the corresponding policies associated with ISG subscriber sessions, also called targets. Each ISG subscriber session can have one or more classifiers associated with it. The different classifiers that can be associated with a subscriber session are:

- Match-Always Classifier—Identifies the entire traffic of a target in a particular direction. A target may have only one match-always classifier in each direction.
- Flow Classifier—Identifies a subset of traffic of a target in a particular direction. A target may have any number of flow classifiers in each direction.
- Default Classifier—Identifies the traffic of a target that does not match any of the flow classifiers in a particular direction. A target may have only one default classifier in each direction.

A set of features represent a policy attached to a classifier. Two classifiers on a target may have the same policy or different policies attached to it. ISG, however, considers the policy of each classifier to be independent of the other classifiers on a target.

The priority defines the order in which a packet should be subjected to classifiers when multiple classifiers are associated with a target. If no priority is defined, the default value of 0 is assumed and the following rules are used to provide the highest possible classification match:

- order of matching
- priority 0 (or not defined)
- priority 1
- priority 2
- ….

Note If two classifiers have the same priority, the order of association to the subscriber session is the differentiator. It is not recommended to use this method, as different delays can occur in bringing up a service and may cause an incorrect classification.

Traffic Policies

Traffic policies define the handling of data packets. A traffic policy contains a traffic class and one or more features. Whereas you can specify the event that will trigger an ISG control policy, the trigger for a traffic policy is implicit--the arrival of a data packet.

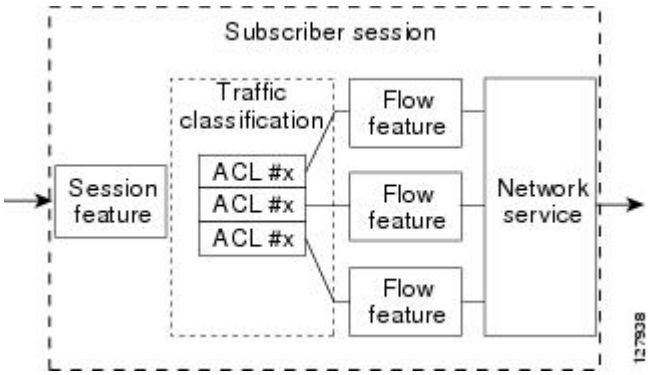
The features configured within a traffic policy apply only to the traffic defined by the traffic class. Multiple traffic policies with various features can be applied to a session.

ISG Features

An ISG feature is a functional component that performs a specific operation on a session's data stream. A feature may or may not be associated with a traffic class. However, once associated with a traffic class, a feature can be applied only to the packets that match that traffic class. Otherwise, the feature is applied to all packets for that session.

The figure below shows how features apply to a subscriber session and to traffic flows within the session.

Figure 63: ISG Feature Application on a Session and Flows



Note Two or more services that specify the same feature and apply to the entire session rather than to a specified traffic flow should not be activated for a session simultaneously. If two or more of these services are activated for a session, deactivation of one of the services will remove the feature from the session. If you need to offer to a subscriber multiple services that specify the same feature and apply to the session rather than a specific flow, configure the services so that they are mutually exclusive. That is, the subscriber should not be able to activate more than one such service at the same time. Similarly, control policies should not activate more than one such service at the same time.

Service Groups

A *service group* is a grouping of services that may be simultaneously active for a given session. Typically, a service group includes one primary service and one or more secondary services.

Secondary services in a service group are dependent on the primary service and should not be activated unless the primary service is already active. Once a primary service has been activated, any other services that reference the same group may also be activated. Services that belong to other groups, however, may be activated only if they are primary. If a primary service from another service group is activated, all services in the current service group will also be deactivated because they have a dependency on the previous primary service.

Service Activation Methods

There are three methods by which services can be activated:

- Automatic service activation
- Control policy service activation
- Subscriber-initiated service activation

Automatic Service Activation

The Auto Service attribute, which can be configured in user profiles, enables subscribers to be automatically logged in to specified services when the user profile is downloaded, usually following authentication. Features that are specified by the Auto Service attribute in a user profile are referred to as *auto services* . A user profile can specify more than one service as auto services.

Control Policy Service Activation

ISG control policies can be configured to activate services in response to specific conditions and events.

Subscriber-Initiated Service Activation

Subscriber-initiated service activation takes place when a subscriber manually selects a service at a portal.

When the system receives a subscriber request to activate a service, the ISG policy engine searches for a policy matching the event “service-start”. If no such policy is found, the policy engine will by default download the service via the default AAA network authorization method list. This default behavior is identical to the behavior generated by the following policy configuration:

```
class-map type control match-all SERVICE1_CHECK
   match service-name SERVICE1
policy-map type control SERVICE1_CHECK event service-start
   1 service-policy type service name SERVICE1
```

The same default behavior applies to subscriber logoffs, with the ISG policy engine searching for a policy that matches the event “service-stop”.

If a policy is configured, it is the responsibility of the policy to specify how the service should be applied.

How to Configure ISG Services on the Router

There are two ways to configure an ISG service. One way is to configure a service policy map on the local device by using the CLI. The second way is to configure a service profile on a remote AAA server. To configure a service policy map directly on the ISG, perform the tasks in the following sections:

Configuring an ISG Service with Per-Session Functionality

Certain types of functionality that are configured in a service must be applied to the entire subscriber session rather than to a specific traffic flow. Services that are configured with this type of per-session functionality must not contain a traffic class. Perform this task to configure a service policy map without a traffic class on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules.

Note A service that is configured with per-session functionality and a traffic policy will not work correctly.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **authenticate aaa list** *name-of-list*
5. **classname** *dhcp-pool-name*
6. **ip portbundle**
7. **ip unnumbered** *interface-type interface-number*
8. **ip vrf forwarding** *name-of-vrf*
9. **service deny**
10. **service relay pppoe vpdn group** *VPDN-group-name*
11. **service vpdn group** *VPDN-group-name*
12. **sg-service-group** *service-group-name*
13. **sg-service-type** {**primary** | **secondary**}

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**authenticate aaa list** *name-of-list* **Example:** `Router(config-service-policymap)# authenticate aaa list mlist`	Indicates that the service requires authentication as a condition of activation and initiates an authentication request.
Step 5	**classname** *dhcp-pool-name* **Example:** `Router(config-service-policymap)# classname green`	Associates a Dynamic Host Configuration Protocol (DHCP) address pool with a service or specific subscriber.
Step 6	**ip portbundle** **Example:** `Router(config-service-policymap)# ip portbundle`	Enables the ISG Port-Bundle Host Key feature in the service policy map.
Step 7	**ip unnumbered** *interface-type interface-number* **Example:** `Router(config-service-policymap)# ip unnumbered ethernet 0`	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 8	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF. • Configuring this command will make the service a primary service.
Step 9	**service deny** **Example:** `Router(config-service-policymap)# service deny`	Denies network service to the subscriber session.
Step 10	**service relay pppoe vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service relay pppoe vpdn group group1`	Enables relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel for a subscriber session.

	Command or Action	Purpose
Step 11	**service vpdn group** *VPDN-group-name* **Example:** `Router(config-service-policymap)# service vpdn group vpdn1`	Provides virtual private dialup network (VPDN) service for ISG subscriber sessions. • Configuring this command will make the service a primary service.
Step 12	**sg-service-group** *service-group-name* **Example:** `Router(config-service-policymap)# sg-service-group group1`	Associates the service with a specified service group.
Step 13	**sg-service-type** {**primary** | **secondary**} **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary or secondary service. • A primary service is a service that contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

Configuring an ISG Service with a Traffic Policy

An ISG traffic policy contains a traffic class and one or more ISG features. The traffic class defines the traffic to which the features will be applied. Perform the following tasks to configure an ISG service with a traffic policy on the router:

Defining an ISG Traffic Class Map

Perform this task to configure a traffic class map. A traffic class map usually specifies an access control list (ACL) that classifies the flow and the direction of traffic to which the ACL applies (inbound or outbound).

Note You can also configure an empty traffic class map, that is, a traffic class map that does not specify an access list, in order to configure a service with a traffic policy that applies to all session traffic.

Before you begin

This task assumes that access control lists (ACLs) have been configured for classifying traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group input** {*access-list-number* | **name** *access-list-name*}
5. **match access-group output** {*access-list-number* | **name** *access-list-name*}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type traffic match-any** *class-map-name* **Example:** `Router(config)# class-map type traffic match-any class1`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class.
Step 4	**match access-group input** {*access-list-number* | **name** *access-list-name*} **Example:** `Router(config-traffic-classmap)# match access-group input 101`	(Optional) Configures the match criteria for an input class map on the basis of the specified ACL. • Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.
Step 5	**match access-group output** {*access-list-number* | **name** *access-list-name*} **Example:** `Router(config-traffic-classmap)# match access-group output 102`	(Optional) Configures the match criteria for an output class map on the basis of the specified ACL. • Skip this step if you want to define a traffic policy that applies to all session traffic rather than to a specific traffic flow.
Step 6	**exit** **Example:** `Router(config-traffic-classmap)# exit`	Returns to global configuration mode.

Configuring an ISG Service Policy Map with a Traffic Policy

ISG services are configured by creating service policy maps on the ISG or service profiles on an external AAA server. Perform this task to configure a traffic policy in a service policy map on the ISG.

Note Some of the commands that can be configured in a service policy map require other configuration in order to work properly. Details on how to configure specific ISG features and functionality are provided in other modules in the *Cisco IOS Intelligent Services Gateway Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **police** {**input** | **output**} *committed-rate normal-burst excess-burst*
7. **prepaid config** *name-of-configuration*
8. **redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*]
9. **timeout absolute** *duration-in-seconds*
10. **timeout idle** *duration-in-seconds*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic classb`	Associates a traffic class map with the service policy map. • The *priority* argument determines which traffic class will be used first for a specified match. When a packet matches more than one traffic class, it is classified to the class with the higher priority.
Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Router(config-service-policymap-class-traffic)# accounting aaa list mlist1`	Enables accounting and specifies the AAA method list to which accounting updates will be sent.
Step 6	**police** {**input**	**output**} *committed-rate normal-burst excess-burst* **Example:**	Enables ISG policing for upstream or downstream traffic. • This command can be entered twice to configure upstream and downstream policing.

	Command or Action	Purpose
	`Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	
Step 7	**prepaid config** *name-of-configuration* **Example:** `Router(config-service-policymap-class-traffic)# prepaid config conf-prepaid`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.
Step 8	**redirect** [**list** *access-list-number*] **to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]} [**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.
Step 9	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout absolute 30`	Specifies the session lifetime, in a range from 30 to 4294967 seconds.
Step 10	**timeout idle** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000`	Specifies how long a connection can be idle before it is terminated. The range is platform and release-specific. For more information, use the question mark (?) online help function.
Step 11	**end** **Example:** `Router(config-service-policymap-class-traffic)#end`	(Optional) Returns to privileged EXEC mode.

Configuring the Default Class in an ISG Service Policy Map

Packets that do not match any traffic classes are considered to be part of default traffic and are processed as if a traffic policy were not applied to the session. A default class exists by default for every service, and the default action of the default class is to pass traffic. Perform this task to configure the default class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic default** {**in-out** | **input** | **output**}
5. **drop**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	**class type traffic default** {**in-out** | **input** | **output**} **Example:** `Router(config-service-policymap)# class type traffic default in-out`	Associates a default traffic class with a service policy map. • The default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.
Step 5	**drop** **Example:** `Router(config-service-policymap-class-traffic)# drop`	Configures the default traffic class to discard packets matching that class.

Activating ISG Subscriber Services

There are three ways that ISG subscriber services can be activated: by specifying the service as an automatic activation service in a subscriber's user profile, by configuring control policies to activate the service, and by a subscriber-initiated service logon. No special configuration is necessary to enable a subscriber to log on to a service.

To configure a service for automatic activation and to configure control policies to activate services, perform the following tasks:

Configuring Automatic Service Activation in a User Profile

Perform this task to configure automatic service activation for a service in a subscriber's user profile.

SUMMARY STEPS

1. Add the Auto Service attribute to the user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Auto Service attribute to the user profile. **Example:** `26,9,251="A service-name[; username ; password]"`	Automatically logs the subscriber in to the specified service when the user profile is downloaded.

Configuring ISG Control Policies to Activate Services

Perform this task to configure a control policy to activate a service.

Before you begin

A control class map must be configured if you specify a named control class map in the control policy map. See the module "Configuring ISG Control Policies" for information about configuring control policies.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**]
5. *action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policy1`	Creates or modifies a policy map to specify an ISG control policy.

	Command or Action	Purpose
Step 4	**class type control** {**always** | *map-class-name*} [**event account-logon** | **credit-exhausted** | **quota-depleted** | **service-start** | **service-stop** | **session-default-service** | **session-service-found**| **session-start** | **timed-policy-expiry**] **Example:** `Router(config-control-policymap)# class type control always event session-start`	Specifies a class and, optionally, an event for which actions may be configured.
Step 5	*action-number* **service-policy type service** {**name** | **unapply**} *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service service1`	Applies the specified service policy map. • To remove the service policy map, use the **unapply** keyword.

Verifying ISG Services

Perform this task to verify ISG service configuration.

SUMMARY STEPS

1. **enable**
2. **show class-map type traffic**
3. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show class-map type traffic** **Example:** `Router# show class-map type traffic`	Displays all traffic class maps and their matching criteria.
Step 3	**show policy-map type service** **Example:** `Router# show policy-map type service`	Displays the contents of all service policy maps.

Configuration Examples for ISG Services

Example Service for Per-Flow Accounting

In the following examples, the service “SERVICE1” is configured with per-flow accounting. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two alternative methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
```

Example Service for Absolute Timeout and Idle Timeout

In the following examples, the service “SERVICE1” is configured with per-flow accounting, an absolute timeout, and an idle timeout. The access lists “SERVICE1_ACL_IN” and “SERVICE1_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any SERVICE1_TC
 match access-group input name SERVICE1_ACL_IN
 match access-group output name SERVICE1_ACL_OUT
!
policy-map type service SERVICE1
 10 class type traffic SERVICE1_TC
  timeout idle 600
  timeout absolute 1800
  accounting aaa list CAR_ACCNT_LIST
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name SERVICE1_ACL_IN priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name SERVICE1_ACL_OUT priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = ISERVICE1
  session-timeout = 1800
  idle-timeout = 600
```

Example Service for ISG Policing

In the following examples, the service “BOD1M” is configured with per-flow accounting and ISG policing. The access lists “BOD1M_IN_ACL_IN” and “BOD1M_ACL_OUT” are used to define the traffic class. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
class-map type traffic match-any BOD1M_TC
 match access-group input name BOD1M_IN_ACL_IN
 match access-group output name BOD1M_ACL_OUT
!
policy-map type service BOD1M
 10 class type traffic BOD1M_TC
  accounting aaa list CAR_ACCNT_LIST
  police input 512000 256000 5000
  police output 1024000 512000 5000
 class type traffic default in-out
  drop
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = "ip:traffic-class=in access-group name BOD1M_IN_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=in default drop"
 Cisco-AVPair = "ip:traffic-class=out access-group name BOD1M _OUT_ACL priority 10"
 Cisco-AVPair = "ip:traffic-class=out default drop"
 Cisco-AVPair = subscriber:accounting-list=CAR_ACCNT_LIST
 Cisco-SSG-Service-Info = IBOD1M
 Cisco-SSG-Service-Info = QU;512000;256000;5000;D;1024000;512000;5000
```

Example Service for Per-Subscriber Firewall

In the following examples, the service “SERVICE2” is configured with a per-subscriber firewall. The service does not include a traffic class, so it will apply to the entire session. These examples are equivalent and show the two methods of service configuration: in a service policy map that is configured directly on the ISG, and in a service profile that is configured on a AAA server.

ISG Configuration

```
policy-map type service SERVICE2
```

```
 ip access-group INTERNET_IN_ACL in
 ip access-group INTERNET_OUT_ACL out
```

AAA Server Configuration

```
Attributes/
 Cisco-AVPair = ip:inacl=INTERNET_IN_ACL
 Cisco-AVPair = ip:outacl=INTERNET_OUT_ACL
```

Example Service for Redirecting Layer 4 Subscriber Traffic

The following example shows the configuration of a service called “UNAUTHORIZED_REDIRECT_SVC”. The control policy “UNAUTHEN_REDIRECT” is configured to apply the service upon session start.

```
class-map type traffic match-any UNAUTHORIZED_TRAFFIC
 match access-group input 100

policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class type traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080

policy-map type control UNAUTHEN_REDIRECT
 class type control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
```

Example Deactivating a Layer 4 Redirection Service Following Authorization

In the following example, a service configured with Layer 4 redirection is deactivated when traffic becomes authorized; that is, following activation of the appropriate service.

```
class-map traffic UNAUTHORIZED_TRAFFIC
match access-group input 100
policy-map type service UNAUTHORIZED_REDIRECT_SVC
 class traffic UNAUTHORIZED_TRAFFIC
  redirect to ip 10.0.0.148 port 8080
class-map control match-all CHECK_ISP1
 match service ISP1
policy-map control UNAUTHEN_REDIRECT
 class control always event session-start
  1 service-policy type service name UNAUTHORIZED_REDIRECT_SVC
 class control CHECK_ISP1 event service-start
  1 service-policy type service unapply UNAUTHORIZED_REDIRECT_SVC
  1 service-policy type service name ISP1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

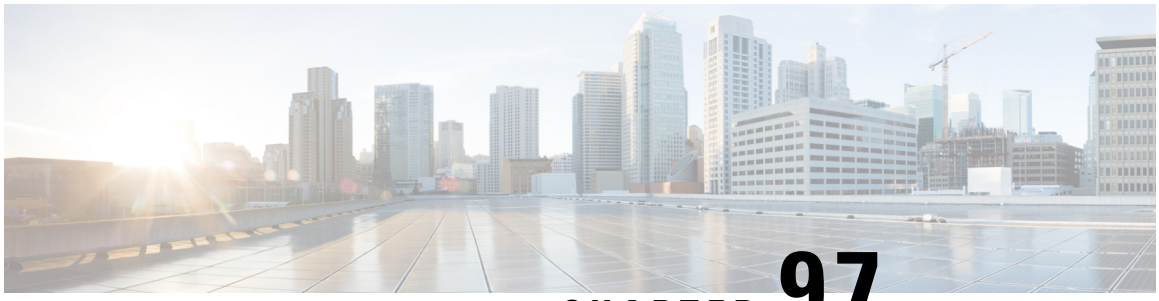
Feature Information for ISG Subscriber Services

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 129: Feature Information for ISG Subscriber Services

Feature Name	Releases	Feature Configuration Information
ISG: Policy Control: Service Profiles	Cisco IOS XE Release 2.2	ISG defines a service as a collection of policies that can be applied to any subscriber session. Services can be configured on the router or on an external AAA server.
ISG: Policy Control: User Profiles	Cisco IOS XE Release 2.2	ISG user profiles specify services and functionality that can be applied to ISG sessions for the specified subscriber. User profiles are defined on an external AAA server.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.3S	ISG no longer creates separate sessions for each traffic class; the traffic class is handled as a flow within the parent subscriber session. The following commands were introduced or modified: **debug subscriber classifier**, **debug subscriber feature**, **show subscriber service**, **show subscriber statistics**.



CHAPTER 97

Configuring ISG Network Forwarding Policies

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. An ISG network forwarding policy is a type of traffic policy that allows packets to be routed or forwarded to and from an upstream network. This module provides information about how to configure network forwarding policies.

Restrictions for ISG Network Forwarding Policies

A service can contain only one network forwarding policy.

For each subscriber session, only one instance of a network forwarding policy can be in effect at any one time.

Information About ISG Network Policies

Network Policies

For subscriber packets to reach a network, some form of forwarding must be specified for a subscriber session. A traffic policy that allows packets to be routed or forwarded to and from an upstream network is known as a *network forwarding policy* .

Where the network forwarding policy type is routing, forwarding decisions are made at Layer 3, and a VRF (Virtual Routing and Forwarding) identifier must be specified to indicate which routing table should be used to make the routing decision (each VRF represents an independent routing context within a single router). Where the network policy type is forwarding, forwarding decisions are made at Layer 2, which means that all subscriber packets are forwarded to and from a single virtual endpoint within the system. This virtual endpoint represents a Layer 2 tunnel, and a tunnel identifier determines which tunnel should be used. If a network forwarding policy is not specified, the global routing table will be used to route traffic.

An ISG service that includes a network forwarding policy is known as a *primary service* . Primary services are mutually exclusive and may not be active simultaneously. Upon activation of a new primary service, ISG will deactivate the existing primary service and any other services dependent on the existing primary service through association with a service group.

Configuration Sources for Network Policies

Network policies can be configured in user profiles and service profiles on an external authentication, authorization, and accounting (AAA) server or in service policy maps on the ISG-enabled device. A network forwarding policy configured in a user profile takes precedence over a network forwarding policy specified in a service.

If a network forwarding policy is not specified in a user profile or service, the ISG session will inherit the network service from another source. ISG can inherit a network service from the following sources:

- Global
- Interface
- Subinterface
- Virtual template

These configuration sources are listed in order of precedence. For example, a network forwarding policy that is configured for a virtual template takes precedence over a network forwarding policy that is configured on an interface.

For each subscriber session, only one instance of a network forwarding policy can be in effect at any point in time.

How to Configure ISG Network Policies

Configuring Network Policies for PPP Sessions in Service Policy Maps

Network policies can be configured in user profiles or service profiles on an external AAA server or in a service policy map on the ISG device. Perform this task to configure a network forwarding policy for PPP sessions in a service policy map on the ISG device.

Note If a network forwarding policy is not specified in a user profile, service profile, or service policy map, a subscriber session will inherit the network forwarding policy from another source. See the "Configuration Sources for Network Policies" section for more information.

Before you begin

This task assumes that virtual private dial up network (VPDN) groups have been configured.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. Do one of the following:
   - **service vpdn group** *vpdn-group-name*
   - **service local**
   - **service relay pppoe vpdn group** *vpdn-group-name*
5. **ip vrf forwarding** *name-of-vrf*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.

Step 4	Do one of the following:
	• **service vpdn group** *vpdn-group-name*
	• **service local**
	• **service relay pppoe vpdn group** *vpdn-group-name*
	Example:
	`Router(config-service-policymap)# service vpdn group vpdn1`
	Example:
	`Router(config-service-policymap)# service local`
	Example:
	`Router(config-service-policymap)# service relay pppoe vpdn group vpdn1`
		Provides virtual private dialup network (VPDN) service.
		or
		Provides local termination service.
		or
		Provides VPDN service by relaying PPPoE over VPDN L2TP tunnels.
		• If you terminate the service locally by configuring the **service local** command, you can also specify the routing domain in which to terminate the session by configuring the **ip vrf forwarding** command.

Step 5	**ip vrf forwarding** *name-of-vrf* **Example:**	Associates the service with a VRF. • Perform this step only if you configured the **service local** command in Step 4. If you configured the **service**

	Command or Action	Purpose
	`Router(config-service-policymap)# ip vrf forwarding blue`	**local** command, you can use the**ip vrf forwarding** command to specify the routing domain in which to terminate session. If you do not specify the routing domain, the global VRF will be used.

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Network Policies for IP Sessions in Service Policy Maps

Network policies can be configured in user profiles or service profiles on an external AAA server or in a service policy map on the ISG device. Perform this task to configure a network forwarding policy for IP sessions in a service policy map on the device.

Note If a network forwarding policy is not specified in a user profile, service profile, or service policy map, a subscriber session will inherit the network forwarding policy from another source. See the "Configuration Sources for Network Policies" section for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:**	Creates or modifies a service policy map, which is used to define an ISG service.

	Command or Action	Purpose
	`Router(config)# policy-map type service service1`	
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** `Router(config-service-policymap)# ip vrf forwarding blue`	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** `Router(config-service-policymap)# sg-service-type primary`	Defines the service as a primary service. • A primary service is a service that contains a network forwarding policy. A primary service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuration Examples for ISG Network Policies

Network Forwarding Policy for PPP Sessions Example

The following example shows a service policy map configured with a network forwarding policy for PPP sessions:

```
policy-map type service my_service
 service vpdn group vpdn1
```

Network Forwarding Policy for IP Sessions Example

The following example shows a service policy map configured with a network forwarding policy for IP sessions:

```
policy-map type service my_service
 ip vrf forwarding vrf1
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
VPDN configuration tasks	*Cisco IOS VPDN Technologies Configuration Guide*
PPP and VPDN commands	*Cisco IOS VPDN Technologies Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Network Policies

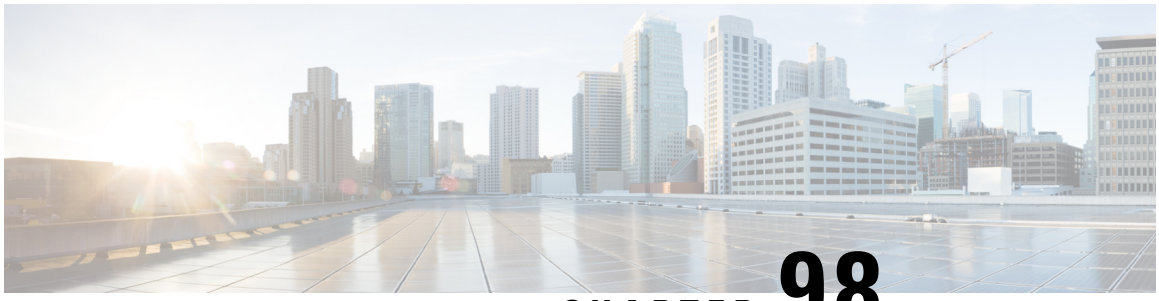
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 130: Feature Information for ISG Network Forwarding Policies

Feature Name	Releases	Feature Configuration Information
ISG: Network Interface: IP Routed, VRF-Aware MPLS	Cisco IOS XE Release 2.2	ISG supports multiple forwarding types to connect sessions to networks. These connections can be to the Internet, corporate intranets, ISPs, or walled gardens for content delivery. ISG supports both routed and MPLS-enabled interfaces for network access.

Feature Name	Releases	Feature Configuration Information
ISG: Network Interface: Tunneled (L2TP)	Cisco IOS XE Release 2.2	ISG is flexible to support multiple interface types to connect sessions to networks. These connections can be to the Internet, corporate intranets, ISPs or walled gardens for content delivery. ISG supports tunneled interfaces to networks.



CHAPTER 98

Configuring ISG Accounting

The Intelligent Services Gateway (ISG) is a Cisco software feature set that provides a structured framework to edge devices that can deliver flexible and scalable services to subscribers. This module describes how to configure ISG accounting, including per-session accounting or per-flow accounting, broadcast accounting, and postpaid tariff switching.

Prerequisites for ISG Accounting

- Configure the authentication, authorization, and accounting (AAA) method list using the **aaa accounting** command before configuring Intelligent Services Gateway (ISG) accounting. ISG sends accounting records to the AAA method list specified in the user profile, service profile, or service policy map. For more information about the AAA commands, see the *Cisco IOS Security Command Reference: Commands A to C* .
- AAA servers must be configured to support ISG accounting.

Restrictions for ISG Accounting

- Intelligent Services Gateway (ISG) accounting supports only the RADIUS protocol.
- If authentication, authorization, and accounting (AAA) broadcast accounting is used with periodic accounting, you cannot configure different accounting periods for different accounting groups.

Information About ISG Accounting

Overview of ISG Accounting

Intelligent Services Gateway (ISG) supports per-session, per-service, or per-flow accounting. Per-session accounting is the aggregate of all the flow traffic for a session and it can be enabled in a user profile.

Per-flow accounting, which accounts for a subset of session traffic as defined by a traffic class, is enabled in a service profile or service policy map. When per-flow accounting is configured, the Parent-Session-ID vendor-specific attribute (VSA) is included in accounting records so that per-session and per-flow accounting records can be correlated in the RADIUS server.

Within a subscriber session, per-service accounting enables RADIUS to track services when they become active and when they stop. Per-service accounting is the aggregate of all flow traffic for the duration of the service. Using this feature, the device includes all activated services for the session in a single accounting start message. Per-service accounting can be enabled in a service profile or service policy map. When per-service accounting is configured, the service name and Parent-Session-ID attributes are included in accounting records.

Note When accounting is configured in a user profile, the service name attribute is not included in accounting records.

Session accounting is enabled if the **aaa accounting network default** command is configured and a authentication, authorization, and accounting (AAA) method list is specified. We recommend that you use a named method list rather than the default method list. Flow accounting is disabled by default and will take place only if a AAA method list is specified in the service profile or a service policy map. ISG accounting sends Accounting-Start, interim, and Accounting-Stop records to the specified AAA method list.

ISG Accounting Messages on ANCP Ports

Accounting messages sent by Intelligent Services Gateway (ISG) for sessions on an Access Node Control Protocol (ANCP) port contain the following authentication, authorization, and accounting (AAA) attributes:

- nas-rx-speed
- nas-rx-speed-bps
- nas-tx-speed
- nas-tx-speed-bps

ISG retrieves the values for these attributes from the Digital Subscriber Line Access Multiplexer (DSLAM) ANCP notification sent to ISG or from the quality of service (QoS) policy configured on the interface.

When an ANCP port is in an up state, the attribute values are taken from the DSLAM ANCP notification sent to ISG. If the ANCP port state changes to a down state, the ANCP accounting messages will continue to contain the AAA attributes sent in the DSLAM notification.

If the ANCP port state has never been set to up, ISG can retrieve the nas-tx-speed, nas-tx-speed-bps, nas-rx-speed, and nas-rx-speed-bps AAA attributes from the QoS policy on that interface.

To retrieve the AAA attributes from the QoS policy, the policy must be configured before the configuration of the ANCP neighbor; otherwise, ISG uses the previous values (if any) for the AAA attributes when a session is established.

If the QoS policy values are changed, ISG continues to use the previous values until the ANCP neighbor is removed and reconfigured.

Service Activation and Deactivation Configuration on RADIUS

You can configure Cisco VSA 250 and VSA 252 in the service profile on RADIUS to dynamically activate and deactivate services. RADIUS uses VSA 250 in Access-Accept and VSA 252 in Change of Authorization (CoA) messages. These VSAs have the following syntax:

```
252 0b "service(parameter1=value,parameter2=value,...)"
250 "service(parameter1=value,parameter1=value,...)"
```

When deactivating a service, RADIUS sends the same information in VSA 252 that was used for service activation, except that service deactivation uses 0c parameters in the VSA instead of the 0b parameter used for service activation. VSA 252 has the following syntax for service deactivation:

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

ISG Accounting Records

Intelligent Services Gateway (ISG) accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based authentication, authorization, and accounting (AAA) server or a mediation server. ISG sends accounting records with the associated attributes to the AAA accounting method list when the following events occur—account logon, account logoff, service logon, and service logoff. The accounting server can be configured to interpret the accounting records to generate bills for postpaid sessions.

Account Logon and Logoff

ISG sends a RADIUS Accounting-Request record to the specified AAA method list when a subscriber logs on to or out off ISG. The Acct-Status-Type attribute included in the Accounting-Request record indicates if the record marks the start (commencement) of the subscriber session or the stop (termination) of the session.

When the **aaa accounting** command is enabled with the **system**, **default**, **start-stop**, and **group** keywords, accounting records are sent to the AAA server. When a subscriber logs on, ISG sends an Accounting-Start record to the AAA server. When a subscriber logs off, ISG sends an Accounting-Stop record to the AAA server.

Service Logon and Logoff

ISG sends a RADIUS Accounting-Start record to the AAA server when a service is activated for a subscriber, and it sends an Accounting-Stop record when a service is deactivated. The record contains an accounting session ID that is different from the accounting session ID of the parent session.

The Acct-Status-Type attribute included in the Accounting-Request record indicates whether the record marks the start or the end of the service. The name of the service is included in accounting records for service logon and logoff.

Accounting records may be sent for events other than account and service logon and logoff. See the *Securing User Services Configuration Guide Library* for more information.

Interim ISG Accounting Updates

Intelligent Services Gateway (ISG) supports interim (intermittent) RADIUS accounting updates that work the same way as "watchdog" RADIUS accounting. Accounting updates are sent between the time that ISG sends Accounting-Start and Accounting-Stop records.

ISG supports two types of interim accounting—accounting updates for new information (such as a new IP address) and periodic accounting, in which accounting records are sent at a configurable interval.

Interim accounting can be enabled or disabled globally for new information. Periodic accounting can be enabled for specific contexts, such as globally, in user profiles, and in services.

Broadcast Accounting

Intelligent Services Gateway (ISG) supports authentication, authorization, and accounting (AAA) broadcast accounting, which is the ability to send user accounting records to multiple RADIUS servers. AAA broadcast accounting provides service providers with geographical redundancy for RADIUS servers and provides accounting records to partners in wholesale models. For information about configuring AAA broadcast accounting, see the "Configuring Accounting" chapter in the *Cisco Authentication, Authorization, and Accounting Configuration Guide.*

ISG Postpaid Tariff Switching

The Intelligent Services Gateway (ISG) Postpaid Tariff Switching feature allows changes in tariffs during the lifetime of a connection. This feature applies to time-based or volume-based postpaid sessions in which the tariff changes at certain times of the day.

Typically, a service provider would use postpaid tariff switching to offer different tariffs to a subscriber while the subscriber is still connected. For example, changing a subscriber to a less expensive tariff during off-peak hours.

To handle tariff switches for postpaid connections, accounting packets log the usage information during the various tariff-switch intervals. The service profile contains a weekly tariff-switch plan detailing the times of day during which tariff changes occur. ISG monitors the usage at every tariff-switch point and records this information in interim accounting records. The billing server monitors all the interim accounting updates and obtains the information about the traffic sent at each tariff rate.

Note Tariff switching is not required for time-based billing services. Because the billing server knows the service logon and logoff time stamps, it can calculate the various tariffs that apply during that time.

Subscriber Accounting Accuracy

The Subscriber Accounting Accuracy feature guarantees that the I/O packet/byte statistics in the Accounting-Stop record are accurate to within one second.

Subscriber accounting data is sent to authentication, authorization, and accounting (AAA) servers during the following events:

- Configured intervals during the lifetime of the session or service

- Service logoff
- Session tear down

Use the **subscriber accounting accuracy** *milliseconds* command to set the value for the Subscriber Accounting Accuracy feature.

HA Support for ISG Accounting

The accounting start and stop records that Intelligent Services Gateway (ISG) sends to an external RADIUS accounting server contains cumulative counters associated with subscriber sessions. ISG can also send interim accounting records containing the latest time and volume statistics at periodic intervals during a session's lifetime. This information is correlated by a third-party billing software to generate billing records for the subscriber.

The ISG stateful switchover (SSO) and In Service Software Upgrade (ISSU) feature adds high availability (HA) support to the ISG session, service, and flow accounting. This HA support includes a periodic session update feature that enables ISG to retain cumulative accounting counters associated with the subscriber sessions after an SSO or ISSU event. Configuring this feature prevents the new active processor from restarting the accounting counters from zero after an SSO event. You can also specify that the first record sent after an SSO event is an interim accounting record for sessions, services, and flows that survive the switchover.

The following are some of the counters and their associated counters that retain their value after Route Processor (RP) SSO:

- Session counters:
  - Acct-Input-Octets
  - Acct-Input-Packets
  - Acct-Output-Octets
  - Acct-Output-Packets
  - Acct-Session-Time
- Service counters:
  - Acct-Input-Octets
  - Acct-Input-Packets
  - Acct-Output-Octets
  - Acct-Output-Packets

For information about configuring HA on the ISG device, see the *High Availability Configuration Guide*.

How to Configure ISG Accounting

Enabling ISG per-Session Accounting

Per-session accounting can be configured in the user profile of a authentication, authorization, and accounting (AAA) server.

This task contains the following sections:

Enabling ISG per-Session Accounting in a User Profile on a AAA Server

Use the attributes given in this procedure to enable per-session accounting in a user profile on an authentication, authorization, and accounting (AAA) server.

Note You must configure a service for an accounting list before enabling a per-session accounting in a user profile. A per-session accounting list cannot be applied on a session in Intelligent Services Gateway (ISG) if a service is not configured; that is, you must have a dummy service configured under the accounting list when there is no service configured.

SUMMARY STEPS

1. Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-Attribute-Value pair (AVpair)="accounting-list=*accounting-mlist-name*"

Adds the Accounting attribute to the user profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the Acct-Interim-Interval (attribute 85) to the user profile. This attribute specifies the number of seconds between interim updates.

Enabling a per-User Accounting List

Perform this task to enable a dummy service on an accounting list. A dummy service is a string that is used to get an authorization from a server for a user profile when no service is configured.

SUMMARY STEPS

1. userxxx2@cisco.com Cleartext-Password := "cisco111"
2. Cisco-Account-Info += "ADUMMYSERVICE",

DETAILED STEPS

Step 1 userxxx2@cisco.com Cleartext-Password := "cisco111"

Adds the username and password account information for a RADIUS user profile.

Step 2 Cisco-Account-Info += "ADUMMYSERVICE",

Adds a dummy service to a RADIUS user profile for an accounting list on an authentication, authorization, and accounting (AAA) server.

Enabling ISG per-Flow Accounting

Intelligent Services Gateway (ISG) per-flow accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

Perform this task to configure a per-flow accounting in a service profile on the authentication, authorization, and accounting (AAA) server.

Before you begin

This task assumes that you have defined IP access lists for specifying the traffic.

SUMMARY STEPS

1. Cisco-AVpair="ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"
2. Cisco-AVpair="accounting-list=*accounting-mlist-name*"
3. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-AVpair="ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

Adds the Intelligent Services Gateway (ISG) traffic class attribute to the service profile. This attribute specifies the input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

Step 2 Cisco-AVpair="accounting-list=*accounting-mlist-name*"

Adds the accounting attribute to the service profile on the AAA server. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent. The AAA method list must be configured.

Note If this attribute is configured in a service profile that does not include a traffic class, accounting is performed on the session rather than on the flow.

Step 3 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the IETF RADIUS attribute Acct-Interim-Interval (attribute 85) to the service profile on the AAA server. This attribute specifies the number of seconds between interim updates.

Enabling ISG per-Flow Accounting in a Service Policy Map

Perform this task to enable accounting in a local service policy map for the device for a specific flow.

Before you begin

This task assumes that you have defined a traffic class map and associated IP access lists. See the module "Configuring ISG Subscriber Services" for more information about configuring traffic classes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **class type traffic** *class-map-name*
5. **accounting aaa list** *AAA-method-list*
6. **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	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service service1`	Creates or defines a service policy map, which is used to define an Intelligent Services Gateway (ISG) service and enters service policy-map configuration mode.
Step 4	**class type traffic** *class-map-name* **Example:** `Device(config-service-policymap)# class type traffic firstclass`	Associates a previously configured traffic class with the policy map and enters control policy-map traffic class configuration.
Step 5	**accounting aaa list** *AAA-method-list* **Example:** `Device(config-control-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent. • The AAA method list must be configured.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-control-policymap-class-traffic)# end`	Returns to privileged EXEC mode.

Enabling ISG per-Service Accounting

Per-service accounting can be configured in the following configuration sources:

- Service profile on a AAA server
- Service policy map on the ISG device

This procedure contains the following sections:

Enabling per-Service Accounting on ISG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber service multiple-accept**
4. **subscriber service session-accounting**
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	**subscriber service multiple-accept** **Example:** `Device(config)# subscriber service multiple-accept`	Enables multiple services in a single Access-Accept message.
Step 4	**subscriber service session-accounting** **Example:**	Enables subscriber services accounting.

	Command or Action	Purpose
	`Device(config)# subscriber service session-accounting`	• All started services are included in the session accounting start message.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Enabling per-Service Accounting in a Service Profile on a AAA Server

Use the attributes in this procedure to enable per-service accounting in a service profile on a authentication, authorization, and accounting (AAA) server. Note that for per-service accounting, the traffic class attribute should not be included in the service profile.

SUMMARY STEPS

1. Cisco-AVpair="accounting-list=*accounting_mlist_name*"
2. IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

DETAILED STEPS

Step 1 Cisco-AVpair="accounting-list=*accounting_mlist_name*"

Adds the Accounting attribute to the service profile. This attribute enables accounting and specifies the AAA method list to which accounting updates will be sent.

Step 2 IETF RADIUS attribute Acct-Interim-Interval (attribute 85)

(Optional) Adds the Acct-Interim-Interval (attribute 85) to the service profile. This attribute specifies the number of seconds between interim updates.

Enabling per-Service Accounting in a Service Policy Map

To configure a per-service accounting in a service policy map on the device, you must configure an empty traffic class map (a traffic class map that does not specify an access list) and enable accounting within the empty traffic class in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **exit**
5. **policy-map type service** *policy-map-name*
6. **class type traffic** *class-map-name*
7. **accounting aaa list** *AAA-method-list*

8. **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	**class-map type traffic match-any** *class-map-name* **Example:** `Device(config)# class-map type traffic match-any empty_class`	Creates or modifies a traffic class map, which is used for matching packets to a specified ISG traffic class, and enters traffic class-map configuration mode. • For per-session accounting, create an empty traffic class map, that is, a traffic class map that does not specify an access list for matching traffic.
Step 4	**exit** **Example:** `Device(config-traffic-classmap)# exit`	Exits traffic class-map configuration mode.
Step 5	**policy-map type service** *policy-map-name* **Example:** `Device(config)# policy-map type service polmap1`	Creates or defines a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 6	**class type traffic** *class-map-name* **Example:** `Device(config-service-policymap)# class type traffic empty_class`	Associates a traffic class map with the service policy map and enters service policy-map traffic class configuration mode. • In this step, reference the empty traffic class map that you created in Step 3.
Step 7	**accounting aaa list** *AAA-method-list* **Example:** `Device(config-service-policymap-class-traffic)# accounting aaa list list1`	Enables accounting and specifies the authentication, authorization, and accounting (AAA) method list to which accounting updates will be sent.
Step 8	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-service-policymap-class-traffic)# end`	

Configuring ISG Postpaid Tariff Switching

ISG postpaid tariff switching can be configured in the service profile on a authentication, authorization, and accounting (AAA) server.

If you include a traffic class in the service profile, postpaid tariff switching will apply to the specified flow. If you do not configure a traffic class, postpaid tariff switching will apply to the session. Perform this task to configure per-session or per-flow postpaid tariff switching.

Before you begin

Intelligent Services Gateway (ISG) per-session or per-flow accounting must be configured for postpaid tariff switching to work.

SUMMARY STEPS

1. Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"
2. Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

DETAILED STEPS

Step 1 Cisco-AVpair = "PPW*hh*:*mm*:*ss*:*d*"

Adds the postpaid VSA to the service profile. This attribute specifies the weekly tariff-switch points for postpaid tariff switching. The syntax description is as follows:

hh :*mm*:*ss*:*d*—Weekly tariff-switch time.

- hh = hour of day <0-23>
- mm = minutes <0-59>
- ss = seconds <0-59>
- d = bitmap format for the days of week. Each weekday is represented by one bit, as follows:
  - 00000001 = Monday
  - 00000010 = Tuesday
  - 00000100 = Wednesday
  - 00001000 = Thursday
  - 00010000 = Friday
  - 00100000 = Saturday
  - 01000000 = Sunday

Step 2 Cisco-AVpair = "ip:traffic-class={in | out} access-group [*acl-number* | name *acl-name*] [priority *n*]"

Adds the ISG traffic class attribute to the service profile. This attribute specifies input and output traffic to which the service will apply. Both an input and output traffic classifier can be added to a service profile.

What to Do Next

You may want to configure a method of activating the service policy map or service profile. For example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Verifying ISG Accounting and Postpaid Tariff Switching

To verify and troubleshoot Intelligent Services Gateway (ISG) accounting and postpaid tariff switching, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

SUMMARY STEPS

1. **show subscriber session**
2. **show aaa sessions**
3. **show aaa user** {**all** | *unique id*}
4. **show sss session** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show subscriber session** **Example:** `Device# show subscriber session`	Displays ISG subscriber session information.
Step 2	**show aaa sessions** **Example:** `Device# show aaa sessions`	Displays authentication, authorization, and accounting (AAA) subscriber session information.
Step 3	**show aaa user** {**all** | *unique id*} **Example:** `Device# show aaa user all`	Displays AAA subscriber information for all users or a specified user.
Step 4	**show sss session** [**all**] **Example:** `Device# show sss session`	Displays Subscriber Service Switch (SSS) session status.

Enabling Periodic Session Update

Perform this task to enable Intelligent Services Gateway (ISG) to periodically synchronize the dynamic accounting statistics (counters) for subscriber sessions on the standby processor, to suppress accounting on and accounting off messages during a switchover, or to send the interim accounting record first after a switchover.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy dynamic periodic-update interval** *minutes*
4. **aaa accounting redundancy suppress system-records**
5. **aaa accounting redundancy best-effort-reuse send-interim**
6. **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	**subscriber redundancy dynamic periodic-update interval** *minutes* **Example:** `Device(config)# subscriber redundancy dynamic periodic-update interval 30`	Enables periodic update of accounting statistics for subscriber sessions.
Step 4	**aaa accounting redundancy suppress system-records** **Example:** `Device(config)# aaa accounting redundancy suppress system-records`	Suppresses accounting on and accounting off messages during a switchover.
Step 5	**aaa accounting redundancy best-effort-reuse send-interim** **Example:** `Device(config)# aaa accounting redundancy best-effort-reuse send-interim`	Sends the interim accounting record first after a switchover for session and service accounting.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying Periodic Session Update

To verify and troubleshoot the configuration of the periodic session update on the ISG device, use any of the following commands in privileged EXEC mode. You can use these commands in any order.

Command	Purpose
show ccm clients	Displays information about cluster control manager (CCM) clients in HA dual RP systems.
show ccm queues	Displays CCM queue statistics for HA dual RP systems.
show ccm sessions	Displays information about CCM sessions in HA dual RP systems.

Troubleshooting ISG Accounting

Use the commands in this task to monitor and troubleshoot Intelligent Services Gateway (ISG) accounting. All these commands are optional and can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **debug radius brief**
4. **debug subscriber feature name accounting event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa accounting** **Example:** `Device# debug aaa accounting`	Displays information about authentication, authorization, and accounting (AAA) TACACS+ authentication.
Step 3	**debug radius brief** **Example:**	Enables debugging of the RADIUS configuration.

	Command or Action	Purpose
	`Device# debug radius brief`	
Step 4	**debug subscriber feature name accounting event** **Example:** `Device# debug subscriber feature name accounting event`	Displays diagnostic information about the installation and removal of ISG features on ISG subscriber sessions.

Configuration Examples for ISG Accounting

Example: Enabling ISG per-Flow Accounting

Example: Enabling ISG per-Flow Accounting in a Service Profile on the AAA Server

The following example shows Intelligent Services Gateway (ISG) per-flow accounting configured in a remote service profile for a service called “video1”:

```
video1        Password = "cisco"
Cisco-AVpair = "traffic-class=input access-group 101 priority 20",
Cisco-AVpair = "traffic-class=output access-group 112 priority 20",
Cisco-Avpair = "accounting-list=remote-local",
Service-Info = "QU;8000",
Service-Info = "QD;64000"
```

Example: Enabling ISG per-Flow Accounting in a Service Policy Map

The following example shows ISG per-flow accounting configured in a service policy map for a service called “video1”:

```
class-map type traffic match-any video1
 match access-group output 101
 match access-group input 100
!
policy-map type service video1
 class type traffic video1
  accounting aaa list mlist1
```

Example: Enabling ISG per-Service Accounting

The following configuration example allows multiple services in a single Access-Accept message and enables session accounting for services. The example also shows how to enable RADIUS to authorize the subscriber to access services.

```
subscriber service multiple-accept
subscriber service session-accounting
subscriber authorization enable
```

Example: Enabling a per-User Accounting List

The following example shows a dummy service configured for an Intelligent Services Gateway (ISG) per-session accounting list configured on an authentication, authorization, and accounting (AAA) server:

```
userxxx2@cisco.com Cleartext-Password := "cisco111"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 192.168.17.17,
         Cisco-Account-Info += "ADUMMYSERVICE",

DUMMYSERVICE Cleartext-Password := "cisco"
         Cisco-AVPair+= "accounting-list=testacct",
```

Example: Enabling ISG per-Service Accounting in a Service Policy Map

The following example shows how to configure per-service accounting in a service policy map on the Intelligent Services Gateway (ISG) device:

```
class-map type traffic match-any classmap1
!
policy-map type service polmap1
 class type traffic classmap1
  accounting aaa list mlist1
```

Example: Configuring Postpaid Tariff Switching

The following example shows the configuration of a postpaid tariff switch each day of the week at midnight:

```
Cisco-AVpair = "PPW00:00:00:127"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 8:00 p.m.:

```
Cisco-AVpair = "PPW20:00:00:31"
```

The following example shows the configuration of a postpaid tariff switch Monday through Friday at 6:00 a.m.:

```
Cisco-AVpair = "PPW06:00:00:31"
```

Example: Enabling Periodic Session Update

The following example shows that the Intelligent Services Gateway (ISG) device is configured to suppress accounting on and accounting off messages during a switchover and to send the interim accounting record first after a switchover. The ISG device also synchronizes the accounting counters for subscriber sessions on the standby processor every 30 minutes.

```
subscriber redundancy dynamic periodic-update interval 30
!
```

```
aaa accounting redundancy suppress system-records
aaa accounting redundancy best-effort-reuse send-interim
```

Examples: Verifying ISG Accounting and Postpaid Tariff Switching

This section contains examples of output for the "Verifying ISG Accounting and Postpaid Tariff Switching" task.

show subscriber session Output When ISG Accounting Is Applied to a Flow

In the following example, Intelligent Services Gateway (ISG) accounting is configured in a service profile that specifies a traffic class, which means that accounting will be performed on the flow and not the parent session. In this example, 157 is the unique ID of the traffic class.

```
Device# show subscriber session uid 157 detailed

Subscriber session handle: E5000092, state: connected, service: Ltm Internal
Unique Session ID: 157
Identifier:
SIP subscriber access type(s): Traffic-Class
Root SIP Handle: 2B000011, PID: 76
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 45 seconds, Last Changed: 3 minutes, 45 seconds
AAA unique ID: 0
Switch handle: F300015F
Session inbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
 Packets = 84, Bytes = 33600


Feature: Policing
 Upstream Params:
Average rate = 8000, Normal burst = 1500, Excess burst = 3000
Config level = Service
Session outbound features:
Feature: Service accounting
 Service: video1
 Method List: remote-local
 Outbound direction:
        Packets = 84, Bytes = 33600
Feature: Policing
 Dnstream Params:
Average rate = 64000, Normal burst = 12000, Excess burst = 24000
Config level = Service
Configuration sources associated with this session:
Service: video1, Active Time = 3 minutes, 46 seconds
```

show subscriber session Output When ISG Accounting Is Applied to a Session

The following is sample output from the **show subscriber session** command for a session rather than a flow:

```
Device# show subscriber session uid 730 detailed

Subscriber session handle: 3800009A, state: connected, service: Local Term
Unique Session ID: 730
Identifier: igq2acct
```

```
SIP subscriber access type(s): IP-Interface/Account-Logon-CH
Root SIP Handle: A600000E, PID: 75
Child SIP Handle: F9000018, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 3 minutes, 57 seconds, Last Changed: 2 minutes, 59 seconds
AAA unique ID: 81
Switch handle: 890003A0
Interface: ATM6/0.1
Policy information:
  Authentication status: authen
  Config downloaded for session policy:
  From Access-Type: Account-Logon-CH, Client: SM, Event: Got More Keys
    Profile name: apply-config-only, 2 references
      ssg-account-info     "SAfoo"
  Rules, actions and conditions executed:
    subscriber rule-map rule1
      condition always event any-event
        action 1 authenticate
Session inbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Session outbound features:
Feature: Session accounting
 Method List: foo
 Outbound direction:
        Packets = 10, Bytes = 1000
Configuration sources associated with this session:
Interface: ATM6/0.1, Active Time = 3 minutes, 58 seconds
```

The following is sample output from the **show aaa sessions** command:

```
Device# show aaa sessions

Total sessions since last reload: 141
Session Id: 167
   Unique Id: 151
   User Name: *not available*
   IP Address: 192.168.0.1
   Idle Time: 0
   CT Call Handle: 0
```

Output for a Specific User

The following is sample output from the **show aaa user** command:

```
Device# show aaa user

Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
```

```
1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
```

```
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Output for All Users

```
Device# show aaa user all

-------------------------------------------------
Unique id 151 is currently in use.
Accounting:
  log=0x20C201
  Events recorded :
    CALL START
    NET UP
    IPCP_PASS
    INTERIM START
    VPDN NET UP
  update method(s) :
    PERIODIC
  update interval = 60
Outstanding Stop Records : 0
  Dynamic attribute list:
    1A1CABE8 0 00000001 connect-progress(68) 4 Call Up
    1A1CABF8 0 00000001 pre-session-time(294) 4 0(0)
    1A1CAC08 0 00000001 nas-tx-speed(421) 4 423630024(194014C8)
    1A1CAC18 0 00000001 nas-rx-speed(71) 4 139317740(84DD1EC)
    1A1CAC28 0 00000001 elapsed_time(364) 4 46122(B42A)
    1A1CAC50 0 00000001 bytes_in(135) 4 11434660(AE7AA4)
    1A1CAC60 0 00000001 bytes_out(274) 4 0(0)
    1A1CAC70 0 00000001 pre-bytes-in(290) 4 0(0)
    1A1CAC80 0 00000001 pre-bytes-out(291) 4 0(0)
    1A1CAC90 0 00000001 paks_in(136) 4 92215(16837)
    1A1CADF0 0 00000001 paks_out(275) 4 0(0)
    1A1CAE00 0 00000001 pre-paks-in(292) 4 0(0)
    1A1CAE10 0 00000001 pre-paks-out(293) 4 0(0)
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=000000A7 Unique Id=00000097
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=189F046C : Name = CAR_mlist
    Attribute list:
      1A1CADF0 0 00000001 session-id(361) 4 167(A7)
1A1CAE00 0 00000001 protocol(297) 4 ip
      1A1CAE10 0 00000001 addr(8) 4 192.168.0.1
      1A1CAE20 0 00000001 Framed-Protocol(101) 4 PPP
      1A1CAE30 0 00000009 clid-mac-addr(37) 6 00 00 04 00 00 2A
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type 8
  No data for type CALL
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  No data for type 12
  No data for type IPSEC-TUNNEL
```

```
  No data for type RESOURCE
  No data for type 15
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
Start Bytes In = 0             Start Bytes Out = 0
    Start Paks  In = 0             Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0             Pre Bytes Out = 0
    Pre Paks  In = 0             Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 11434660      Bytes Out = 0
    Paks  In = 92215         Paks  Out = 0
  StartTime = 12:02:40 IST Oct 16 2007
  AuthenTime = 12:02:40 IST Oct 16 2007
  Component = IEDGE_ACCOUNTING
Authen: service=NONE type=NONE method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000097
  Session Id = 000000A7
  Attribute List:
    1A1CADF0 0 00000001 port-type(198) 4 PPPoE over VLAN
    1A1CAE00 0 00000009 interface(194) 7 4/0/0/2
PerU: No data available
```

Example: Troubleshooting ISG Accounting

The following is sample output from the **debug aaa accounting** command:

```
Device# debug aaa accounting

16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet address=209.165.201.1 cmd=glare bytes_in=308
 bytes_out=76 paks_in=45
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
AAA configuration tasks	*Authentication, Authorization, and Accounting Configuration Guide*

Related Topic	Document Title
AAA commands	*Cisco IOS Security Command Reference: Commands A to C*
Configuring ISG subscriber services	"Configuring ISG Subscriber Services" section in the *Intelligent Services Gateway Configuration Guide*
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS XE High Availability Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Accounting

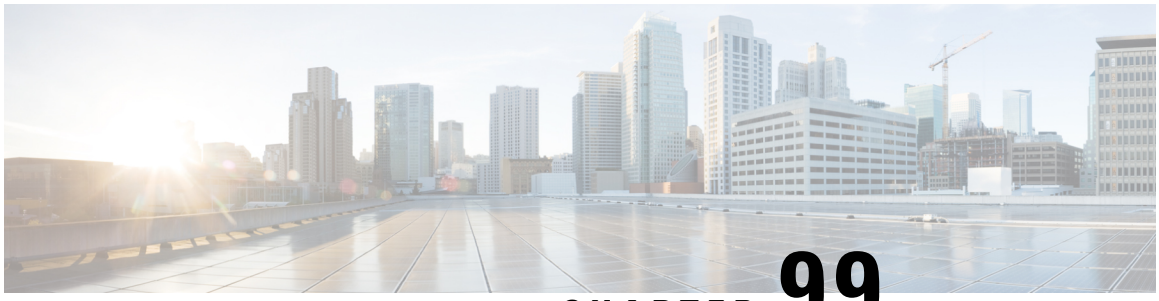
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 131: Feature Information for ISG Accounting

Feature Name	Releases	Feature Information
1 second accuracy—IPv6 session counters and ISGv6 services	Cisco IOS XE Release 3.5S	Support for PPP IPv6 and dual-stack sessions was added to the Subscriber Accounting Accuracy feature.
ISG Accounting—Postpaid	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG sends accounting start and accounting stop records for sessions and services to an accounting server for postpaid billing. The accounting server interprets the records to generate bills.
ISG Accounting—per-Service Accounting	Cisco IOS XE Release 2.4	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server.

Feature Name	Releases	Feature Information
ISG Accounting—Tariff Switching	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. Where billing rates change at fixed times and sessions are active across the boundary at which the rates change, ISG will provide accounting data to the billing server indicating the boundary.
ISG Flow Control—SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for ISG features including ISG accounting.



CHAPTER 99

Configuring ISG Support for Prepaid Billing

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG prepaid billing support allows an ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG prepaid billing works on a repeated re-authorization model in which fragments of credit, called *quotas*, are allotted by a prepaid billing server. This model allows a subscriber to be connected to multiple simultaneous prepaid services, each with a different billing rate. ISG supports time-based and volume-based prepaid billing.

This module describes how to configure ISG support for prepaid billing for IPv4, IPv6 and dual-stack sessions.

Prerequisites for ISG Prepaid Billing Support

- A subscriber session is created and a method of service activation is in place.
- Traffic classes for IPv4, IPv6, and dual-stack sessions are configured.
- A global IPv6 address is necessary for the session to function properly.

Restrictions for ISG Prepaid Billing Support

- ISG prepaid billing support can only be applied to traffic flows that have been defined by an ISG traffic class.
- ISG prepaid billing support can not be applied to per-user ACL on IPv6 traffic.
- Quotas are measured in seconds for time and in bytes for volume. There is no way to change the unit of measure.

- The volume quota is for combined upstream and downstream traffic.
- The volume quota supports a maximum value of 4 GB.
- PREPIAD (TC service) does not support services with a link local IPv6 address after IPCPv6 negotiation. A global IPv6 address is required for the session to function properly.
- IPv6 prefix delegation works independently through DHCPv6 and its transparency to ISG sessions. DHCPv6 assigns IPv6 addresses using either **ipv6 local pool** or **framed-ipv6-prefix** with RADIUS.

Information About ISG Prepaid Billing Support

Overview of ISG Support for Prepaid Billing

ISG prepaid billing is supported for IPv4, IPv6, and dual-stack subscribers. This feature allows ISG to check the subscriber's available credit to determine whether to activate a specified service and how long the session can last. The subscriber's credit is administered by a prepaid billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A *quota* is an allotment, or fragment, of available credit. Allocating quotas in fragments rather than providing all the credit at once enables ISG to support the use of credit for multiple simultaneous prepaid sessions.

ISG uses the RADIUS protocol to facilitate interaction between ISG and external authentication, authorization, and accounting (AAA) servers and prepaid billing servers. A single device can serve as the AAA server and the billing server.

To obtain the first quota for a session, ISG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to ISG. ISG then monitors the session to track the quota usage. When the quota runs out or a specified limit is reached, ISG performs re-authorization. During re-authorization, the prepaid billing server may provide ISG with an additional quota if there is available credit. If no further quota is provided, ISG will log the user off from the service or perform some other specified action.

When a service is deactivated, the cumulative usage is provided to the prepaid billing server in an Accounting-Stop message.

ISG Prepaid Volume Monitor Polling Timer and QV Values

The Cisco IOS prepaid volume monitor polling timer determines when ISG will initiate a prepaid reauthorization. The polling timer value is (15 seconds < polling-monitor-time < 300 seconds). This value is calculated dynamically based on the QV value (which defines the volume-based quota), the actual rate, and the configured volume threshold. The prepaid volume monitor polling timer is not directly configurable.

To avoid allocating more volume quota than the subscriber is entitled to during the first authorization (when usage rate is unknown), the QV value should be a minimum of (15 x access rate). In cases in which the usage rate is known, the QV value should be at least (15 x usage rate).

In cases in which the input access rate is much higher than the QV value, it is recommended that the correct QV value be calculated using the following formula: access rate x 15 > QV < access rate x 300. For example, an ADSL2 or VDSL user access-rate can be up to 20 Mbps. That is approximately 2.5 megabytes (MB) of data in one second. Calculate the QV value by using the following formula: 2.5 MB x 15 seconds > QV < 2.5 MB x 300 seconds. This calculation results in a QV value between 37.5 MB and 750 MB, however we

recommend you do not choose either the highest or lowest value in this range. For example, you might pick a value of QV = 100 MB.

ISG Prepaid Threshold

By default, ISG sends reauthorization requests to the billing server when a subscriber's quota is exhausted. ISG prepaid thresholds allow ISG to send reauthorization requests before a quota is used up. When a prepaid threshold is configured, ISG sends a reauthorization request to the billing server when the amount of remaining quota is equal to the value of the threshold. Prepaid thresholds can be configured for both time and volume.

For example, if the prepaid threshold is configured for 10 seconds, and the prepaid billing server sends ISG a quota of 30 seconds, ISG will send a reauthorization request to the prepaid billing server when the subscriber has used up 20 seconds of the quota and has 10 seconds remaining.

ISG Prepaid Idle Timeout

The ISG prepaid idle timeout can be used to suspend a prepaid service session if no traffic is received for a specified period of time. ISG keeps the session up during the suspension but releases all quota previously received for the prepaid session. Subsequent traffic on the session will cause ISG to send a reauthorization request and download a new quota for the session.

Benefits of ISG Prepaid Billing

Concurrent Prepaid Service Access

The ISG Support for Prepaid Billing feature is capable of supporting concurrent prepaid service access while maintaining the same pool of quota at the prepaid billing server. ISG services can be configured for concurrent or sequential access. Concurrent access allows users to log on to a service while simultaneously connected to other services.

Real-Time Billing

The ISG Support for Prepaid Billing feature allows for real-time billing with maximum flexibility, regardless of the type of service and billing scheme. Users can be billed on a flat rate, air-time, or volume basis.

Redirection Upon Exhaustion of Quota

When a user runs out of quota, ISG can redirect the user to a portal where the user can replenish the quota without being disconnected from the service.

Returning Residual Quota

ISG can return residual quota to the billing server from services that a user is logged into but not actively using. The quota that is returned to the billing server can be applied to other services that the user is actively using.

Threshold Values

ISG enables you to configure threshold values that cause prepaid sessions to be reauthorized before the subscriber completely consumes the allotted quota for a service.

Traffic Status During Reauthorization

You can prevent revenue leaks by configuring ISG to drop connected traffic during reauthorization of a service. The user remains connected to the service and does not need to log in to the service again, but no traffic is forwarded during the reauthorization process. This prevents a user from continuing to use a service for which the user has run out of quota while ISG sends a reauthorization request to the billing server.

Simultaneous Volume-Based and Time-Based Prepaid Billing

ISG supports rating on both time and volume simultaneously for prepaid services. The prepaid billing server may allocate quotas in both time and volume, and ISG monitors the session on both these parameters. ISG performs a reauthorization whenever either of these quota types is exhausted.

How to Configure ISG Support for Prepaid Billing

Configuring RADIUS Attribute Support for ISG Prepaid Billing

Perform this task to enable ISG to include RADIUS attribute 44 in Access-Request packets and attribute 55 in Accounting-Request packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]
4. **radius-server attribute 55 include-in-acct-req**
5. **end**
6. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*] **Example:** `Router(config)# radius-server attribute 44 include-in-access-req`	Sends RADIUS attribute 44 (Accounting Session ID) in Access-Request packets before user authentication.

	Command or Action	Purpose
Step 4	**radius-server attribute 55 include-in-acct-req** **Example:** `Router(config)# radius-server attribute 55 include-in-acct-req`	Sends the RADIUS attribute 55 (Event-Timestamp) in Accounting-Request packets.
Step 5	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Creating an ISG Prepaid Billing Configuration

Perform this task to create or modify an ISG prepaid billing configuration. This configuration can be referenced in service profiles or service policy maps in which ISG prepaid support is enabled.

A default prepaid configuration exists with the following parameters:

```
subscriber feature prepaid default
 threshold time 0 seconds
 threshold volume 0 bytes
 method-list authorization default
 method-list accounting default
 password cisco
```

The default configuration will not show up in the output of the **show running-config** command unless you change any one of the parameters.

The parameters of named prepaid configurations are inherited from the default configuration, so if you create a named prepaid configuration and want only one parameter to be different from the default configuration, you have to configure only that parameter.

Before you begin

This task assumes that AAA method lists, server groups, and servers have been configured. See the Cisco IOS Security Configuration Guide: Securing User Services for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber feature prepaid** {*name-of-config* | **default**}
4. **interim-interval** *number-of-minutes*
5. **method-list** {**accounting** | **authorization**} *name-of-method-list*

6. **password** *password*
7. **threshold** {**time** *seconds* | **volume** {*kilobytes* **Kbytes** | *megabytes* **Mbytes** | *bytes* **bytes**}}
8. **end**
9. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber feature prepaid** {*name-of-config*	**default**} **Example:** `Router(config)# subscriber feature prepaid conf-prepaid`	Creates a new ISG prepaid configuration or specifies an existing configuration so it can be modified, and enters prepaid configuration mode.
Step 4	**interim-interval** *number-of-minutes* **Example:** `Router(config-prepaid)# interim-interval 5`	Enables interim prepaid accounting and specifies the interval at which ISG will send interim prepaid accounting records.
Step 5	**method-list** {**accounting**	**authorization**} *name-of-method-list* **Example:** `Router(config-prepaid)# method-list accounting list1`	Specifies the AAA method list to be used for ISG prepaid accounting or authorization.
Step 6	**password** *password* **Example:** `Router(config-prepaid)# password cisco`	Configures the password to be used for ISG prepaid authorization and reauthorization requests.
Step 7	**threshold** {**time** *seconds*	**volume** {*kilobytes* **Kbytes**	*megabytes* **Mbytes**	*bytes* **bytes**}} **Example:** `Router(config-prepaid)# threshold time 20`	Configures the threshold at which ISG will send a reauthorization request to the prepaid billing server. • The quota provided by the billing server minus the configured threshold equals the value at which ISG will send a reauthorization request • This command can be entered twice to configure thresholds in both time and volume.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(config-prepaid)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 9	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Enabling ISG Prepaid Billing

Perform one of the following tasks to enable prepaid billing in a service policy map or a remote service profile:

Enabling ISG Prepaid Billing in a Service Policy Map

Perform this task to enable ISG prepaid billing support in a service policy map.

Before you begin

ISG prepaid billing is enabled in a traffic class within a service policy map. This task assumes that you have defined the traffic class map and associated IP access lists. See the module "Configuring ISG Subscriber Services" for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **prepaid config** *name-of-configuration*
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service mp3`	Creates or defines a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic class-acl-101`	Associates a previously configured traffic class with the policy map, and enters control policy-map traffic class configuration mode.
Step 5	**prepaid config** *name-of-configuration* **Example:** `Router(config-control-policymap-class-traffic)# prepaid config conf-prepaid`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters. **Note** The presence of this command does not guarantee that prepaid billing will be applied to the flow. This command causes the first prepaid authorization request. Whether prepaid billing will be applied to the flow is determined by the billing server.
Step 6	**end** **Example:** `Router(config-control-policymap-class-traffic)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Enabling ISG Prepaid Billing in Service Profile on the AAA Server

Perform this task to enable ISG support for prepaid billing in a service profile that is configured on a remote AAA server.

SUMMARY STEPS

1. Do one of the following:
   - Add the ISG Traffic Class attribute to the service profile.

- Cisco-AVpair = "ip:traffic-class=in access-group [<acl_number> | name <acl_name>] [priority <n>]"
- Cisco-AVpair = "ip:traffic-class=out access-group [<acl_number> | name <acl_name>] [priority <n>]"

2. Add the ISG Prepaid Billing VSA to the service profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Add the ISG Traffic Class attribute to the service profile. • Cisco-AVpair = "ip:traffic-class=in access-group [<acl_number> | name <acl_name>] [priority <n>]" • Cisco-AVpair = "ip:traffic-class=out access-group [<acl_number> | name <acl_name>] [priority <n>]"	Specifies input and output traffic to which the service will apply. • Both an input and output traffic classifier can be added to a service profile.
Step 2	Add the ISG Prepaid Billing VSA to the service profile. **Example:** `26,9,1 = "prepaid-config={<name-of-config> | default"`	Enables ISG support for prepaid billing and applies a configuration that defines the prepaid billing parameters.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Redirecting Subscriber Traffic upon Exhaustion of Credit

Service providers often want to offer subscribers an opportunity to recharge their accounts when they have run out of credit for their prepaid services. The tasks in this section enable you to redirect a subscriber's Layer 4 traffic to a specified server when the subscriber has run out of credit.

Before you configure ISG Layer 4 Redirect for exhaustion of credit, you should understand the following concept:

Perform the following tasks to redirect a subscriber's Layer 4 traffic upon exhaustion of credit:

Credit-Exhausted Event

The ISG credit-exhausted event occurs when the prepaid server responds with an Access-Accept packet with a quota value of zero (time or volume) and an idle timeout greater than zero. In this case, the prepaid server has determined for certain that the subscriber does not have enough credit, but the idle timeout provides a grace period in which the subscriber could recharge the account. Typically, a service provider would want to redirect the subscriber's traffic to a web portal where the subscriber could recharge the account. At the end of the idle-timeout interval, ISG will send a reauthorization request.

The default ISG behavior is to drop subscriber packets when the credit-exhausted event occurs. However, in case of dual-stack subscriber, the ISG redirects the subscriber to the portal in case of credit exhaustion.

Note Layer 4 redirection is one action that a service provider could take when a subscriber has run out of credit. Other actions can be configured instead of or in addition to Layer 4 redirection.

Configuring L4 Redirection in a Service Policy Map

Perform this task to configure ISG Layer 4 redirection in a service policy map.

The ISG Layer 4 Redirect feature can also be configured in a service profile on a AAA server. For more information about redirecting Layer 4 subscriber traffic, see the "Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module.

Before you begin

The ISG Layer 4 Redirect feature is configured under a traffic class within the service policy map. This task assumes that you have defined the traffic class map. See the "Configuring ISG Subscriber Services" module for more information.

Traffic can be redirected to a server or server group. If you are redirecting traffic to a server group, this task assumes that the server group has been configured. See the "Configuring ISG Subscriber Services" module for more information about configuring server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-name*
5. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*]
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service redirect-service`	Creates or defines a service policy map, which is used to define an ISG service and enters service policy-map configuration mode.
Step 4	[*priority*] **class type traffic** *class-name* **Example:** `Router(config-service-policymap)# class type traffic class-all`	(Optional) Associates a previously configured traffic class with the policy map, and enters service policy-map traffic class configuration mode.
Step 5	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to group redirect-sg`	Redirects traffic to a specified server or server group.
Step 6	**end** **Example:** `Router(config-control-policymap-class-traffic)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

Applying a Service Policy Map to Subscriber Traffic upon Exhaustion of Credit

Perform this task to configure a control policy and apply a service policy map to subscriber traffic upon exhaustion of credit.

Before you begin

If you specify a named control class map, this task assumes that the class map has been configured. See the "Configuring ISG Control Policies" module for information about configuring control class maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event credit-exhausted**

5. *action-number* **service-policy type service name** *policy-map-name*
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policyA`	Creates or modifies a policy map that defines a control policy.
Step 4	**class type control** {*control-class-name* | **always**} **event credit-exhausted** **Example:** `Router(config-control-policymap)# class type control always event credit-exhausted`	Specifies a control class and event for which actions may be configured.
Step 5	*action-number* **service-policy type service name** *policy-map-name* **Example:** `Router(config-control-policymap-class-control)# 1 service-policy type service name redirect-profile`	Applies the specified service policy map or service profile in which the ISG Layer 4 Redirect feature has been configured.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

What to Do Next

Control policies must be applied to a context by using the **service-policy type control** command.

Forwarding Subscriber Traffic upon Depletion of Quota

By default, ISG drops subscriber packets when a subscriber's quota has been depleted. This task enables you to override the default and forward subscriber traffic when the quota-depleted event occurs.

Before you perform this task you should understand the concept described in the Quota-Depleted Event, on page 1411 section.

Quota-Depleted Event

A quota-depleted event occurs when a subscriber's quota is exhausted and ISG has not yet received a reauthorization response from the billing server. This event can occur in two situations:

- When a prepaid threshold is not configured and the subscriber's quota is used up.
- When a prepaid threshold is configured but the quota is exhausted before the prepaid server responds to the reauthorization request that ISG sent when the threshold was met.

The quota-depleted event is not necessarily an indication that a subscriber does not have any more credit. ISG does not know for certain whether the subscriber has any more credit until a reauthorization response is returned from the billing server. For this reason, some service providers may choose to forward subscriber packets upon quota depletion until a reauthorization response is returned.

The default ISG behavior is to drop subscriber packets when a quota-depleted event occurs.

Before you begin

If you specify a named control class map, this task assumes that the class map has been configured. See the module "Configuring ISG Control Policies" for information about configuring control class maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event quota-depleted**
5. *action-number* **set-param drop-traffic false**
6. **end**
7. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control policyB`	Creates or modifies a policy map that can be applied globally, to an interface, or to an ATM VC to specify a control policy, and enters control policy-map configuration mode.
Step 4	**class type control** {*control-class-name* | **always**} **event quota-depleted** **Example:** `Router(config-control-policymap)# class type control always event quota-depleted`	Specifies a control class and event for which actions may be configured, and enters control policy-map class control configuration mode.
Step 5	*action-number* **set-param drop-traffic false** **Example:** `Router(config-control-policymap-class-control)# 1 set-param drop-traffic false`	Configures ISG to continue to allow traffic to pass when the quota has been depleted.
Step 6	**end** **Example:** `Router(config-control-policymap-class-control)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 7	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	(Optional) Displays ISG subscriber session information.

What to Do Next

Control policies must be applied to a context by using the **service-policy type control** command.

Troubleshooting ISG Prepaid Billing Support

Perform these steps to troubleshoot ISG prepaid billing support.

SUMMARY STEPS

1. Use the **show subscriber session** command to make sure the service in which prepaid billing support is configured has been activated.
2. If the service requires service authentication, make sure the authentication succeeded.

3. Make sure the AAA method list referred to in the prepaid billing configuration is valid and has been configured with the **aaa accounting network** command.
4. Use the **test aaa** command to make sure the AAA server is reachable from ISG.
5. Use the **debug subscriber policy prepaid** command to display debug messages about prepaid operation.

DETAILED STEPS

Step 1 Use the **show subscriber session** command to make sure the service in which prepaid billing support is configured has been activated.

Step 2 If the service requires service authentication, make sure the authentication succeeded.

Step 3 Make sure the AAA method list referred to in the prepaid billing configuration is valid and has been configured with the **aaa accounting network** command.

Step 4 Use the **test aaa** command to make sure the AAA server is reachable from ISG.

Step 5 Use the **debug subscriber policy prepaid** command to display debug messages about prepaid operation.

Configuration Examples for ISG Prepaid Billing Support

ISG Prepaid Billing Support Example

The following example shows ISG prepaid billing support configured with the following parameters:

- The time threshold is 20 seconds.
- The volume threshold is 1000 bytes.
- When the quota-depleted event occurs, ISG will drop subscriber packets until the billing server sends another quota.
- When the credit-exhausted event occurs, subscriber packets will be redirected to the server group “redirect-sg”.
- The prepaid service is called “mp3” and is configured directly on the router in a service policy map.
- The AAA method list that will be used for this service to authenticate subscribers is called “cp-mlist”. That is the same method list to which the service accounting records will be sent.
- Prepaid authorization, reauthorization and accounting messages will be sent to the AAA method list called “ap-mlist”.

```
!
aaa authorization network default local
aaa authorization network ap-mlist group sg2
aaa authentication login cp-mlist group sg1
aaa accounting network cp-mlist start-stop group sg1
aaa accounting network ap-mlist start-stop group sg2
service-policy type control RULEA
!
class-map type traffic match-any CLASS-ALL
!
```

```
class-map type traffic match-any CLASS-ACL-101
    match access-group input 101
!
policy-map type control RULEA
 class type control always event credit-exhausted
  1 service-policy type service name redirectprofile
!
policy-map type service redirectprofile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
policy-map type service mp3
 class type traffic CLASS-ACL-101
  accounting aaa list cp-mlist
 !
 authenticate aaa list cp-mlist
!
subscriber feature prepaid conf-prepaid
 method-list accounting ap-mlist
 method-list authorization default
 password cisco
 threshold time 20
 threshold volume 1000 bytes
```

ISG Policies for Handling Credit-Exhausted and Quota-Depleted Prepaid Billing Events Example

In the following example, a single control policy called “RULEA” has been defined to override the ISG prepaid default behavior by forwarding subscriber packets after a quota-depleted event and redirecting subscriber packets after a credit-exhausted event:

```
!class-map type traffic match-any CLASS-ALL
!
policy-map type control RULEA
 class type control always event quota-depleted
  1 set-param drop-traffic false
 class type control always event credit-exhausted
  1 service-policy type service name l4redirect
!
policy-map type service l4redirect
 class type traffic CLASS-ALL
  redirect to group SESM
!
subscriber feature prepaid conf-prepaid
 threshold time 100
 threshold volume 1000 bytes
 method-list author prepaidlist
 method-list accounting default
 password cisco
```

Example: Configuring Prepaid Support for Simple IP Dual Stack Sessions

```
#--------------------
# AAA Configuration
#--------------------
aaa group server radius PREPAID_V4
server-private 6.6.6.1
!
```

```
aaa group server radius PREPAID_V6
server-private 8.8.8.1
!
aaa group server radius SERVER_GROUP1
server name RAD1
!
aaa authorization network PREPAID_V4 group PREPAID_V4
aaa authorization network PREPAID_V6 group PREPAID_V6
aaa authorization subscriber-service default local group SERVER_GROUP1
#---------------------------
# Prepaid Service Definition
#---------------------------
subscriber feature prepaid V4_PREPAID
threshold time 100 seconds
threshold volume 1000 bytes
interim-interval 2 minutes
method-list author PREPAID
method-list accounting List3
password cisco
!
subscriber feature prepaid V6_PREPAID
threshold time 0 seconds
threshold volume 0 bytes
interim-interval 2 minutes
method-list author PREPAID_V6
method-list accounting List1
password cisco
#-----------------------------
# Redirect Portal Configuration
#-----------------------------
redirect server-group IPv6_PORTAL
server ip 3001::2 port 23
!
redirect server-group IPv4_PORTAL
server ip 4.4.4.1 port 23
#---------------------------
# Traffic Class Configuration
#---------------------------
class-map type traffic match-any IPv4_L4R
match access-group input name ipv4_l4r_in
match access-group output name ipv4_l4r_out
!
class-map type traffic match-any IPv6_L4R
match access-group input name ipv6_l4r_in
match access-group output name ipv6_l4r_out

class-map type traffic match-any IPv4_PRE
match access-group input name ipv4_in
match access-group output name ipv4_out
!
class-map type traffic match-any IPv6_PRE
match access-group input name ipv6_in
match access-group output name ipv6_out

class-map type control match-all PRE_V4
match service-name PREPAID_V4_SERVICE
!
class-map type control match-all PRE_V6
match service-name PREPAID_V6_SERVICE
#-----------------------------------------
# IPv4 and IPv6 Prepaid Service Configuration
#-----------------------------------------
policy-map type service PREPAID_V4_SERVICE
10 class type traffic IPv4_PRE
```

```
  prepaid config V4_PREPAID
!
class type traffic default in-out
  drop
!
policy-map type service PREPAID_V6_SERVICE
10 class type traffic IPv6_PRE
  prepaid config V6_PREPAID
!
class type traffic default in-out
  drop
!
#-------------------------------------
# IPv4 and IPv6 L4R Service Definition
#-------------------------------------
policy-map type service L4REDIRECT_SERVICE_V4
5 class type traffic IPv4_L4R
  redirect to group DASHBOARD
!
class type traffic default in-out
  drop
!
policy-map type service L4REDIRECT_SERVICE_V6
5 class type traffic IPv6_L4R
  redirect to group IPv6_PORTAL
!
class type traffic default in-out
  drop
#-----------------------------
# Service Policy Configuration
#-----------------------------
policy-map type control TAL
class type control PRE_V4 event credit-exhausted
  1 service-policy type service name L4REDIRECT_SERVICE_V4
!
class type control PRE_V6 event credit-exhausted
  1 service-policy type service name L4REDIRECT_SERVICE_V6
!
class type control always event session-start
  9 authorize identifier mac-address
!
class type control always event quota-depleted
  1 set-param drop-traffic TRUE
!
#----------------------------------------
# IPv4 and IPv6 Access Lists Configuration
#----------------------------------------
ip access-list extended ipv4_in
permit ip any 4.4.4.0 0.0.0.255
!
ip access-list extended ipv4_out
permit ip 4.4.4.0 0.0.0.255 any
!
ip access-list extended ipv4_l4r_in
permit tcp any any
permit udp any any
!
ip access-list extended ipv4_l4r_out
permit tcp any any
permit udp any any
!
ipv6 access-list ipv6_in
permit ipv6 any 3001::/64
!
```

```
ipv6 access-list ipv6_out
permit ipv6 3001::/64 any
!
ipv6 access-list ipv6_l4r_in
permit tcp any any
permit udp any any
!
ipv6 access-list ipv6_l4r_out
permit udp any any
permit tcp any any
!
#---------------------------
# RADIUS Server Configuration
#---------------------------
radius-server host 6.6.6.1
radius-server host 8.8.8.1
!
radius server RAD1
address ipv4 4.4.4.1 auth-port 1645 acct-port 1646
```

Additional References

Related Documents

Related Topic	Document Title
AAA configuration tasks	The "Authentication, Authorization, and Accounting (AAA)﷯? section in the*Cisco IOS Security Configuration Guide*
AAA commands	*Cisco IOS Security Command Reference*
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Support for Prepaid Billing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 132: Feature Information for ISG Support for Prepaid Billing

Feature Name	Releases	Feature Configuration Information
ISG: Accounting: Prepaid	Cisco IOS XE Release 2.5.0	ISG prepaid billing support allows ISG to check a subscriber's available credit to determine whether to allow the subscriber access to a service and how long the access can last. ISG supports volume-based and time-based prepaid billing.
Prepaid Support for Dual-Stack Sessions	Cisco IOS XE Release 3.13S	ISG prepaid billing support is extended to dual-stack sessions.

CHAPTER 100

Configuring ISG Policies for Session Maintenance

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure a session timer and connection timer through a service policy map. Additionally, the Internet Engineering Task Force (IETF) RADIUS attributes Session-Timeout (attribute 27) and Idle-Timeout (attribute 28) can be used in service profiles on an authentication, authorization, and accounting (AAA) server to configure the same session maintenance control.

IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed host (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP.

Prerequisites for ISG Policies for Session Maintenance

A traffic class is required only if an idle timer or session timer is being installed on a service that has a traffic class definition in it. If the timer is installed on a session or service that has no traffic class, a traffic class is not required. See the "Configuring ISG Subscriber Services" module for information about how to configure a traffic class.

Information About ISG Policies for Session Maintenance

Session Maintenance Timers

ISG provides two commands (each of which can be set independently) to maintain control over a session and its connection. The **timeout absolute** command controls how long a session can be connected before it is

terminated. The **timeout idle** command controls how long a connection can be idle before it is terminated. Both commands detect both PPP and IP sessions and can be applied in a non-traffic-class-based service, on a per-session basis, or in a flow (traffic-class-based service). All subscriber traffic will reset the timers; however, non-network traffic such as PPP control packets will not reset the timers.

The scope of the session timers and connection timers is determined by the type of service within which the timer is specified. If specified in a service profile for which no traffic class is defined, the timer action will be to terminate the session or connection. If a traffic class specifier resides in the service profile, the timer action will be to deactivate the service.

Benefits of Session Maintenance Timers

The PPP idle timeout functionality has been replaced by the ISG idle timeout feature. The idle timer is a generic feature that can be set to detect idle traffic in both PPP and IP sessions.

You set the idle timer in a service profile that is installed on a session to control how long that service stays installed before it is removed from the session because no traffic is flowing through that service. If the service has traffic class parameters associated with it, that traffic class is terminated when this timer expires, or when the session itself is terminated.

The same is true for the session timer, except that this timer determines how long the session or service stays up, regardless of traffic flowing through it.

Monitoring Sessions

The IP subscriber session's data traffic in the upstream direction can be monitored for idleness using a keepalive feature configured for the subscriber. If a session is idle for a configured period of time, keepalive requests are sent to the subscriber. This action verifies that the connection is still active. The protocol to use for the keepalive request and response can be configured based on the IP subscriber session type. If it is a directly connected host (Layer 2 connection), ARP is used. For routed host (Layer 3 connected) subscribers, ICMP is used. If the access interface does not support ARP, the keepalive protocol defaults to ICMP.

ARP for Keepalive Messages

When a session is established and the keepalive feature is configured to use ARP, the keepalive feature saves the ARP entry as a valid original entry for verifying future ARP responses.

Note In cases where the access interface does not support ARP, the protocol for keepalives defaults to ICMP.

When ARP is configured, the ARP unicast request is sent to the subscriber. After a configured interval of time, the ARP response (if received) is verified. If the response is correct and matches the original entry that was saved when the subscriber was initially established, the keepalive feature continues monitoring the data plane for the configured interval of time. If the response is not correct, the keepalive feature resends the ARP request until a correct response is received or the configured maximum number of attempts is exceeded.

ICMP for Keepalive Messages

If ICMP is configured, the ICMP “hello” request is sent to the subscriber and checked for a response, until the configured maximum number of attempts is exceeded.

For IP subnet sessions, the peer (destination) IP address to be used for ICMP “hello” requests will be all the IP addresses within the subnet. This means “hello” requests will be sent sequentially (not simultaneously) to all the possible hosts within that subnet. If there is no response from any host in that subnet, the session will be disconnected.

Another option is to configure ICMP directed broadcast for keepalive requests. If the subscriber hosts recognize the IP subnet broadcast address, the ISG can send the ICMP “hello” request to the subnet broadcast address. The subscribers need not be on the same subnet as the ISG for this configuration to work. A directed broadcast keepalive request can work multiple hops away as long as these conditions are satisfied:

- The group of subscribers identified by the subnet must have the same subnet mask provisioned locally as the subnet provisioned on the subnet subscriber session on the ISG. Otherwise, the subscriber hosts will not recognize the subnet broadcast address.
- The router directly connected to the hosts must enable directed-broadcast forwarding, so that the IP subnet broadcast gets translated into a Layer 2 broadcast.

When these two conditions are satisfied, you can optimize the ICMP keepalive configuration to minimize the number of ICMP packets.

Note Because enabling directed broadcasts increases the risk of denial of service attacks, the use of subnet directed broadcasts is not turned on by default.

HA Support for Session Maintenance Timers

The SSO and ISSU feature provides high availability (HA) support for ISG timers including the connection timer, session timer, and the session keepalive. The timers and keepalive are restarted on the new standby Route Processor (RP) after a stateful switchover (SSO) or In Service Software Upgrade (ISSU) event.

For information about configuring HA on the ISG router, see the High Availability Configuration Guide, Cisco IOS XE Release 3S .

How to Configure ISG Policies for Session Maintenance

Configuring the session maintenance timers requires two separate tasks, one to set the idle timer and one to set the session timer. Either one or both of these tasks can be performed in order to set session maintenance control. The following tasks show how to set these timers in a service policy map and in a RADIUS AAA server profile:

Configuring the Session Timer in a Service Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic***class-map-name*
5. **timeout absolute** *duration-in-seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policy1`	Enters policy map configuration mode so you can begin configuring the service policy.
Step 4	[*priority*] **class type traffic***class-map-name* **Example:** `Router(config-control-policymap)# class type traffic class1`	Associates a previously configured traffic class with the policy map.
Step 5	**timeout absolute** *duration-in-seconds* **Example:** `Router(config-control-policymap-class-control)# timeout absolute 30`	Specifies the session lifetime, in seconds.
Step 6	**end** **Example:** `Router(conf-subscriber-profile)# end`	Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Session Timer on a AAA Server

Perform this task to configure the session timer in a service profile on a AAA server.

SUMMARY STEPS

1. **Session-Timeout=***duration-in-seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**Session-Timeout=***duration-in-seconds*	Sets the IETF RADIUS session timer (attribute 27) in a user or service profile, in a range from 0 to 31104000 seconds.

Configuring the Connection Timer in a Service Policy Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*] **class type traffic** *class-map-name*
5. **timeout idle** *duration-in-seconds* [**both** | **inbound**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:**	Enters policy map configuration mode so you can begin configuring the service policy.

	Command or Action	Purpose
	`Router(config)# policy-map type service policy1`	
Step 4	[*priority*] **class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic class1`	Associates a previously configured traffic class to the policy map.
Step 5	**timeout idle** *duration-in-seconds* [**both** | **inbound**] **Example:** `Router(config-control-policymap-class-traffic)# timeout idle 3000 inbound`	Specifies how long a connection can be idle before it is terminated and in which direction to apply the timer. The range is platform and release-specific. For more information, use the question mark (?) online help function.
Step 6	**end** **Example:** `Router(config-control-policymap-class-traffic)# end`	Returns to privileged EXEC mode.

What to Do Next

You may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring the Connection Timer on a AAA Server

Perform this task to set the connection timer (idle timeout) in a AAA service profile.

SUMMARY STEPS

1. **idle-timeout=** *duration-in-seconds*
2. **idle-timeout-direction=** *direction*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**idle-timeout=** *duration-in-seconds*	Sets IETF RADIUS attribute 28 in a user or service profile, in a range from 1 to 15552000 seconds.
Step 2	**idle-timeout-direction=** *direction*	Sets the direction of subscriber traffic on which to apply the idle timeout. Values are **inbound** or **both**. If the timer is configured without specifying a direction, it is applied by default to the outbound direction.

Example

```
simulator radius subscriber 999
attribute 28 numeric 100
vsa cisco generic 1 string "subscriber:idle-timeout-direction=inbound"
attribute 44 string "00000008"
```

Verifying the Session and Connection Timer Settings

Perform this task to verify that the timers have been installed correctly.

SUMMARY STEPS

1. **enable**
2. **show subscriber session all**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session all** **Example:** `Router# show subscriber session all`	Displays current subscriber information, including reports about the timers that are enabled.
Step 3	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Troubleshooting the Session and Connection Timer Settings

The following sections describe the **debug** commands that can be used to troubleshoot the session maintenance timers:

Prerequisites for Troubleshooting the Session Maintenance Timers

Before performing the task in this section, it is recommended that you be familiar with the use of Cisco IOS **debug** commands described in the introductory chapters of the *Cisco IOS Debug Command Reference.* Also see the module "Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging."

Restrictions for Troubleshooting the Session Maintenance Timers

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the Cisco IOS **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, we recommend that you use **debug** commands during periods of lower network traffic and fewer users, or on a debug chassis with a single active session. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Debug Commands Available for the Session Maintenance Timers

The table below lists the **debug** commands that can be used to diagnose problems with the session maintenance timers.

Table 133: Debug Commands for Troubleshooting Session Maintenance Timers

Command	Purpose
debug subscriber feature error	Displays general Feature Manager errors.
debug subscriber feature event	Displays general Feature Manager events.
debug subscriber feature name idle-timer error	Displays idle timer errors.
debug subscriber feature name idle-timer event	Displays idle timer events.
debug subscriber feature name session-timer error	Displays session timer errors.
debug subscriber feature name session-timer event	Displays session timer events.

Configuring a Session Keepalive on the Router

This task describes how to configure the keepalive feature on the router, using either ARP or ICMP.

Because the session keepalive feature is checking for the subscriber's health and presence, this feature is applied only to the session as a whole and not per-flow.

Note
- If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.
- If this feature is applied to a non-IP session, for example, a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session, this feature application will fail and the following applies:
  - If the feature is applied at a session-start event, both the feature application and the session will fail.
  - If this feature is pushed onto a session after the session-start event, the push will fail.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service policymap1`	Enters service policy map configuration mode.
Step 4	**keepalive** [**idle** *idle-seconds*] [**attempts** *max-retries*] [**interval** *retry-seconds*] [**protocol** {**ARP** | **ICMP** [**broadcast**]}] **Example:** `Router(config-service-policymap)# keepalive idle 7 attempts 3 interval 1 protocol arp`	Enables keepalive messages and sets the maximum idle period, number of requests, interval between requests, and protocol for keepalive messages. • The ranges and default values for the **idle**, **attempts**, and **interval** keywords are platform and release-specific. For more information, use the question mark (**?**) online help function. • **protocol** —For Layer 2 connections, the default is ARP; for routed connections, the default is ICMP. • **broadcast** —This option is disabled by default. **Note** If this command is applied to a non-IP session, the command will fail. If the command is applied to a non-IP session at the session-start event, the session will also fail.
Step 5	**exit** **Example:** `Router(config-service-policymap)# exit`	Returns to global configuration mode.

Example

The following example configures the keepalive feature on a router using ARP:

```
policy-map type service accting_service
 class type traffic ALL
 !
 keepalive idle 7 attempts 3 interval 1 protocol arp
!
```

Configuring a Session Keepalive on a RADIUS Server

This task describes how to configure the session keepalive parameters on a RADIUS server.

SUMMARY STEPS

1. Service-Name password = “cisco”
2. Cisco-Avpair = “subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}”

DETAILED STEPS

Step 1 Service-Name password = “cisco”

Step 2 Cisco-Avpair = “subscriber:keepalive = [idle *period1*] [attempts *Max-retries*] [interval *period2*] [protocol *ICMP* [broadcast] | *ARP*}”

Configures the allowable idle period, maximum number of attempts to connect, the interval between attempts, and the communication protocol to be used.

The ranges and defaults are as follows:

- Idle period: range is 5 to10 seconds; default is 10 seconds.
- Attempts: range is 3 to 10; default is 5.
- Interval: default is 1 to 10 seconds.
- Protocol: for Layer 2 connections, the default is ARP; for routed connections, the default is ICMP.
- Broadcast option: by default this option is disabled.

Note If a service profile includes an ISG traffic class configuration, the keepalive feature will be ignored.

Configuring the ISG to Interact with the RADIUS Server

The ISG device interacts with the RADIUS server to listen for the Packet of Disconnect (POD) message from the RADIUS server. On receipt, the POD and associated attributes are handed to the appropriate client to disconnect the session. Perform this task to configure the ISG to interact with the RADIUS server to listen for the POD message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** *ip-address*
6. **port** *port-number*
7. **server-key** *word*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa server radius dynamic-author** **Example:** `Router(config)# aaa server radius dynamic-author`	Configures a device as a AAA server to facilitate interaction with an external policy server and enters dynamic authorization local server configuration mode.
Step 5	**client** *ip-address* **Example:** `Router(config-locsvr-da-radius)# client 10.10.10.11`	Specifies a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests. • The example specifies 10.10.10.11 as the IP address of the RADIUS client.
Step 6	**port** *port-number* **Example:** `Router(config-locsvr-da-radius)# port 1650`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. • The example specifies port 1650.
Step 7	**server-key** *word* **Example:** `Router(config-locsvr-da-radius)# server-key abc`	Configures the RADIUS key to be shared between a device and RADIUS clients. • The example specifies “abc” as the encryption key shared with the RADIUS client.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Configuration Examples for ISG Policies for Session Maintenance

Example: Session Timer Configuration in a Service Policy Map

The following example limits session time in a service policy map to 4800 seconds (80 minutes):

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout absolute 4800
 class type traffic default
 drop
```

Example: Connection Idle Timer Configuration in a Service Policy Map

The following example limits idle connection time in a service policy map to 30 seconds:

```
class-map type traffic match-any traffic-class
 match access-group input 101
 match access-group output 102
policy-map type service video-service
 class type traffic traffic-class
  police input 20000 30000 60000
  police output 21000 31500 63000
  timeout idle 30
 class type traffic default
 drop
```

Example: Session Timer Show Command Output

The following example shows the settings for the session timer displayed by the **show subscriber session all** privileged EXEC command:

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 3
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
```

```
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:02:50, Last Changed: 00:02:53
AAA unique ID: 4
Interface: Virtual-Access2.1
Policy information:
  Context 02DE7380: Handle 1B000009
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Non-datapath features:
 Feature: Session Timeout
  Timeout value is 180000 seconds
  Time remaining is 2d01h
Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:02:52
```

Example: Connection Idle Timer Show Command Output

The following example shows the settings for the idle timer as displayed by the **show subscriber session all** privileged EXEC command:

```
Current Subscriber Information: Total sessions 1
------------------------------------------------
Unique Session ID: 4
Identifier: user01
SIP subscriber access type(s): PPPoE/PPP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:01:44, Last Changed: 00:01:46
AAA unique ID: 5
Interface: Virtual-Access2.1

Policy information:
  Context 02DE7380: Handle AD00000C
  Authentication status: authen
  User profile, excluding services:
    Framed-Protocol      1 [PPP]
    username             "user01"
    Framed-Protocol      1 [PPP]
    username             "user01"
  Prepaid context: not present
Session outbound features:
 Feature: PPP Idle Timeout
  Timeout value is 2000
  Idle time is 00:01:44

Configuration sources associated with this session:
Interface: Virtual-Template1, Active Time = 00:01:47
```

Example: Session Timer Debug Output

The following example shows output when the session timer debug commands (**debug subscriber feature error** , **debug subscriber feature event**, **debug subscriber feature name session-timer error** , and **debug subscriber feature name session-timer event**) are enabled:

```
*Jan 12 18:38:51.947: SSF[Vi2.1/Abs Timeout]: Vaccess interface config
```

```
update; not per-user, ignore
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Install interface configured
features
*Jan 12 18:38:53.195: SSF[Vt1/uid:3]: Associate segment element handle
0x95000002 for session 1191182344, 1 entries
*Jan 12 18:38:53.195: SSF[Vt1/uid:3/Abs Timeout]: Group feature install
*Jan 12 18:38:53.195: SSF[uid:3/Abs Timeout]: Adding feature to none segment(s)
```

Example: Connection Idle Timer Debug Output

The following example shows output when the idle timer debug commands (**debug subscriber feature error**, **debug subscriber feature event**, **debug subscriber feature name idle-timer error**, and **debug subscriber feature name idle-timer event**) are enabled:

```
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Install interface configured
features
*Jan 12 18:43:15.167: SSF[Vt1/uid:4]: Associate segment element handle
0xF4000003 for session 67108875, 1 entries
*Jan 12 18:43:15.167: SSF[Vt1/uid:4/Idle Timeout]: Group feature install
*Jan 12 18:43:15.167: SSF[uid:4/Idle Timeout]: Adding feature to outbound
segment(s)
*Jan 12 18:43:15.167: Idle Timeout[uid:4]: Idle timer start, duration 2000
seconds, direction: outbound
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] created
02DFFDD8
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] added
02DFFDD8 [outbound]
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:16.327: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097]
installed: ok
*Jan 12 18:43:19.147: SSM FH: [SSS:PPPoE:8198:Idle Timeout:4097] bound
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
ppp timeout idle and **timeout absolute** PPP timer commands	Cisco IOS Dial Technologies Command Reference
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS High Availability Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Policies for Session Maintenance

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 134: Feature Information for ISG Policies for Session Maintenance

Feature Name	Releases	Feature Information
ISG: Session: Lifecycle: Idle Timeout	Cisco IOS XE Release 2.2	The ISG idle timeout controls how long a connection can be idle before it is terminated.
ISG: Session Protection and Resiliency: Keepalive-ARP, ICMP	Cisco IOS XE Release 2.2	IP subscriber session keepalive support is configured for monitoring session data traffic in the upstream direction for idleness. Address Resolution Protocol (ARP) is used for Layer 2 connected subscribers. For routed hosts (Layer 3 connected) subscribers, the protocol defaults to Internet Control Message Protocol (ICMP). ICMP is also used in configurations where the access interface does not support ARP. The following command was introduced: **keepalive** (ISG).
ISG: Session: Lifecycle: Packet of Disconnect (POD)	Cisco IOS XE Release 2.2	An ISG can be configured to interact with external policy servers. A policy server can use RADIUS Packet of Disconnect (POD) to manage the life cycle of any ISG session. The primary role of the POD message is to terminate an ISG session.
Downstream Idle Timeout Support	Cisco IOS XE Release 3.4.1S	The connection timer (idle timeout) can be applied to subscriber traffic in a specific direction, through an ISG service policy map or a AAA service profile. The following command was modified: **timeout idle**.

Feature Name	Releases	Feature Information
Session Timeout Ext to 360 Days	Cisco IOS XE Release 3.5S	Maximum value of the session timer was increased to 31,104,000 seconds. Maximum value of the connection timer was increased to 15,552,000 seconds. The following commands were modified: **timeout absolute**, **timeout idle**.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for the session maintenance timers and keepalive.

CHAPTER 101

Redirecting Subscriber Traffic Using ISG Layer 4 Redirect

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG to redirect subscriber traffic by using the ISG Layer 4 Redirect feature. The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or UDP packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be used to facilitate subscriber authentication, initial and periodic advertising captivation, redirection of application traffic, and Domain Name System (DNS) redirection.

Restrictions for Redirecting ISG Subscriber Traffic

The ISG Layer 4 Redirect feature applies only to TCP or UDP traffic.

A Layer 4 Redirect feature and a traffic-class (TC) service containing a Layer 4 Redirect feature cannot be applied on the same session. A Layer 4 Redirect feature can be applied on a TC in a service, but not directly on a session.

Information About Redirecting ISG Subscriber Traffic

Overview of ISG Layer 4 Redirect

The ISG Layer 4 Redirect feature redirects specified packets to servers that handle the packets in a specified manner. For example, packets sent upstream by unauthorized users can be forwarded to a server that redirects the users to a login page. Similarly, if users try to access a service to which they have not logged in, the packets can be redirected to a server that provides a service login screen.

The Layer 4 Redirect feature supports three types of redirection, which can be applied to subscriber sessions or to flows:

- Initial redirection—Specified traffic is redirected for a specific duration of the time only, starting from when the feature is applied.
- Periodic redirection—Specified traffic is periodically redirected. The traffic is redirected for a specified duration of time. The redirection is then suspended for another specified duration. This cycle is repeated. During periodic redirect, all new TCP connections are redirected until the duration of the redirect is over. After that time any new incoming TCP connections will not be redirected. However, all existing TCP connections that were initiated during this redirection will still be redirected so as not to break the connections.
- Permanent redirection—Specified traffic is redirected to the specified server all the time.

A redirect server can be any server that is programmed to respond to the redirected packets. If ISG is used with a web portal, unauthenticated subscribers can be sent automatically to a login page when they start a browser session. Web portal applications can also redirect to service login pages, advertising pages, and message pages.

Redirected packets are sent to an individual redirect server or redirect server group that consists of one or more servers. ISG selects one server from the group on a rotating basis to receive the redirected packets.

When traffic is redirected, ISG modifies the destination IP address and TCP port of upstream packets to reflect the destination server. For downstream packets, ISG changes the source IP address and port to the original packet's destination.

When traffic is selected by a policy map that includes a **redirection** command, packets are fed back into the policy map classification scheme for a second service selection. The modified IP headers can be subject to different classification criteria. For example, if two class maps exist, each with different **redirection** commands, packets could be redirected, selected by the first class map, and redirected a second time. To avoid this situation, configure traffic class maps so that two consecutive redirections cannot be applied to the same packet.

Layer 4 Redirect Applications

The Layer 4 Redirect feature supports the following applications:

- TCP redirection for unauthenticated users and unauthorized services—HTTP traffic from subscribers can be redirected to a web dashboard where the subscribers can log in so that authentication and authorization can be performed.
- Initial and periodic redirection for advertising captivation—Subscriber traffic can be redirected to a sponsor's web page for a brief period of time at the start of the session or periodically throughout the session.
- Redirection of application traffic—Application traffic from a subscriber can be redirected so as to provide value-added services. For example, a subscriber's Simple Mail Transfer Protocol (SMTP) traffic can be redirected to a local mail server that can function as a forwarding agent for the mail.
- DNS redirection—DNS queries may be redirected to a local DNS server. In some deployments, such as public wireless LAN (PWLAN) hot spots, subscribers may have a static DNS server addresses, which may not be reachable at certain locations. Redirecting DNS queries to a local DNS server allows applications to work properly without requiring reconfiguration.

HA Support for Layer 4 Redirect

The SSO and In ISSU feature provides high availability (HA) support for the ISG Layer 4 Redirect feature. Layer 4 redirect includes the selected service group in its checkpointed data during the initial session and bulk synchronization. The standby processor uses the service group instead of selecting a new one.

Because Layer 4 redirect translations are maintained on the forwarding processor, the translation entries and associated timers are preserved after a route processor stateful switchover (SSO) or In Service Software Upgrade (ISSU) event. The entries are re-created, however, on the new active processor after a forwarding processor switchover.

For information about configuring HA on the ISG router, see the High Availability Configuration Guide, Cisco IOS XE Release 3S .

How to Configure ISG Layer 4 Redirect

There are three ways to apply Layer 4 redirection to sessions. One way is to configure redirection directly on a physical main interface or logical subinterface. A second way is to configure a service profile or service policy map with the Layer 4 redirect attribute in it, and apply that service to the session. A third way is to configure the Layer 4 redirect attribute in the user profile.

The following tasks describe how to configure Layer 4 redirection. The first task is optional. One or more of the next three tasks is required. The last task is optional.

For examples of Layer 4 redirection configuration for specific applications (such as unauthenticated user redirect), see the "Configuration Examples for ISG Layer 4 Redirect" section.

Defining a Redirect Server Group

Perform this task to define a group of one or more servers to which traffic will be redirected. Traffic will be forwarded to servers on a rotating basis.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect server-group** *group-name*
4. **server ip** *ip-address* **port** *port-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**redirect server-group** *group-name* **Example:** `Router(config)# redirect server-group ADVT-SERVER`	Enters redirect server-group configuration mode to define a group of servers in a named redirection server group.
Step 4	**server ip** *ip-address* **port** *port-number* **Example:** `Router(config-sg-l4redirect-group)# server ip 10.0.0.1 port 8080`	Adds a server to a redirect server group. • You can enter this command more than one time to add multiple servers to the server group.

Configuring Layer 4 Redirection in a Service Policy Map

Perform this task to configure Layer 4 redirection in a service policy map.

Before you begin

The ISG Layer 4 Redirect feature is configured under a traffic class within a service policy map. This task assumes that you have defined the traffic class map. See the "Configuring ISG Subscriber Services" module for more information.

Note Only ISG policing and accounting features can be enabled in conjunction with redirection on the same service policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redirect session-limit** *maximum-number*
4. **policy-map type service** *policy-map-name*
5. **class type traffic** *class-name*
6. **redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**redirect session-limit** *maximum-number* **Example:** `Router(config)# redirect session-limit 5`	(Optional) Sets the maximum number of Layer 4 redirects allowed for each subscriber session.
Step 4	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Enters service policy-map configuration mode to create or modify a service policy map, which is used to define an ISG service.
Step 5	**class type traffic** *class-name* **Example:** `Router(config-service-policymap)# class type traffic class1`	(Optional) Enters traffic class map configuration mode to specify a traffic class map that identifies the traffic to which this service applies.
Step 6	**redirect to** {**group** *server-group-name* | **ip** *ip-address* [**port** *port-number*]}[**duration** *seconds*] [**frequency** *seconds*] **Example:** `Router(config-service-policymap-class-traffic)# redirect to ip 10.10.10.10`	Redirects traffic to a specified server or server group.

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Layer 4 Redirection in a Service Profile or User Profile on the AAA Server

The Layer 4 Redirect feature can be configured as a Cisco vendor-specific attribute (VSA) in a service profile on an authentication, authorization, and accounting (AAA) server. This attribute can appear more than once in a profile to define different types of redirections for a session and can be used in both user and non-TC service profiles simultaneously.

SUMMARY STEPS

1. Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the Layer 4 Redirect VSA to the user profile or subscriber profile on the AAA server. **Example:** `Cisco-AVPair = "ip:l4redirect=redirect to {group server-group-name | ip server-ip-address [port port-number]} [duration seconds] [frequency seconds]"`	Redirects traffic to a specified server or server group.

What to Do Next

If you configure ISG Layer 4 redirection in a service profile, you may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the "Configuring ISG Subscriber Services" module.

Verifying ISG Traffic Redirection

Perform this task to verify the configuration and operation of ISG Layer 4 traffic redirection. The **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show redirect translations** [**ip** *ip-address* | **ipv4** | **ipv6**] [**verbose**]
3. **show redirect group** [*group-name*]
4. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show redirect translations** [**ip** *ip-address* | **ipv4** | **ipv6**] [**verbose**] **Example:** `Router# show redirect translations ip 10.0.0.0`	Displays ISG Layer 4 redirect translations for sessions.
Step 3	**show redirect group** [*group-name*] **Example:** `Router# show redirect group redirect1`	Displays information about ISG redirect server groups.

	Command or Action	Purpose
Step 4	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Examples

The following is sample output from the **show redirect translations** command showing the number of active redirect translations:

```
Router# show redirect translations

Maximum allowed number of L4 Redirect translations per session: 5
Destination IP/port    Server IP/port    Prot  In Flags  Out Flags  Timestamp
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01
10.0.1.2        23     10.0.2.2   23     TCP                      Oct 21 2009 11:48:01
Total Number of Translations: 3
Highest number of L4 Redirect: 3 by session with source IP 10.0.0.2
```

The following sample output from the **show subscriber session** command shows that Layer 4 redirect is being applied from the service profile:

```
Router# show subscriber session uid 135

Subscriber session handle: 7C000114, state: connected, service: Local Term
Unique Session ID: 135
Identifier: blind-rdt
SIP subscriber access type(s): IP-Interface
Root SIP Handle: CF000020, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 40 minutes, 30 seconds, Last Changed: 40 minutes, 30 seconds
AAA unique ID: 135
Switch handle: F000086
Interface: ATM2/0.53
Policy information:
  Authentication status: unauthen
  Config downloaded for session policy:
  From Access-Type: IP-Interface, Client: SM, Event: Service Selection Request, Service
    Profile name: blind-rdt, 2 references
      username             "blind-rdt"
      l4redirect           "redirect to group sesm-grp"
  Rules, actions and conditions executed:
    subscriber rule-map blind-rdt
      condition always event session-start
        action 1 service-policy type service name blind-rdt
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    SVC  Redirect to group sesm-grp  !! applied redirect
Configuration sources associated with this session:
Service: blind-rdt, Active Time = 40 minutes, 32 seconds
Interface: ATM2/0.53, Active Time = 40 minutes, 32 seconds
```

The following is sample output from the **show subscriber session**command for a session in which the Layer 4 redirection is applied on the interface:

```
Router# show subscriber session uid 133

Subscriber session handle: D7000110, state: connected, service: Local Term
Unique Session ID: 133
Identifier:
SIP subscriber access type(s): IP-Interface
Root SIP Handle: 1E, PID: 73
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 42 minutes, 54 seconds, Last Changed: 42 minutes, 54 seconds
AAA unique ID: 133
Switch handle: 17000084
Interface: FastEthernet0/0/0.505
Policy information:
  Authentication status: unauthen
Session inbound features:
 Feature: Layer 4 Redirect
  Rule  Cfg  Definition
  #1    INT  Redirect to group sesm-grp
Configuration sources associated with this session:
Interface: FastEthernet0/0/0.505, Active Time = 42 minutes, 54 seconds
```

Configuration Examples for ISG Layer 4 Redirect

Example: Redirecting Unauthenticated Subscriber Traffic

In the following example, Layer 4 redirection is configured in the service policy map “BLIND-RDT.” This policy is applied to all sessions at session start and redirects subscriber TCP traffic to the server group called “PORTAL.” At account login the subscriber is authenticated and the redirection is not applied.

```
Service-policy type control DEFAULT-IP-POLICY
policy-map type control DEFAULT-IP-POLICY
 class type control always event session-start
  1 service-policy type service name BLIND-RDT
!
 class type control always event account-logon
  1 authenticate aaa list AUTH-LIST
  2 service-policy type service unapply name BLIND-RDT
policy-map type service BLIND-RDT
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
redirect server-group PORTAL
 server ip 2001:ABCD:14::6, Port 8000
```

Example: Redirecting Unauthorized Subscriber Traffic

The following example shows the configuration of redirection for unauthorized subscribers. If the subscriber is not logged into the service called “svc,” traffic that matches “svc” is redirected to the server group “PORTAL.” Once the subscriber logs on to the service, the traffic is no longer redirected. When the subscriber logs off the service, redirection is applied again.

```
service-policy type control THE_RULE
!
class-map type traffic match-any CLASS-ALL
!
class-map type traffic match-any CLASS-100_110
 match access-group input 100
 match access-group output 110
!
policy-map type service blind-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc-rdt
 class type traffic CLASS-ALL
  redirect to group PORTAL
!
policy-map type service svc
 class type traffic CLASS-100_110
 class type traffic default in-out
  drop


policy-map type control THE_RULE
 class type control alwyas event account-logon
  1 authenticate
  2 service-policy type service name svc-rdt
 class type control cond-svc-logon event service-start
  1 service-policy type service unapply name svc-rdt
  2 service-policy type service identifier service-name
 class type control cond-svc-logon event service-stop
  1 service-policy type service unapply name svc
  2 service-policy type service name svc-rdt
 !
class-map type control match-all cond-svc-logon
 match identifier service-name svc
!
redirect server-group PORTAL
 server ip 10.2.36.253 port 80
```

Example: Initial ISG Redirection

The following example shows ISG configured to redirect the Layer 4 traffic of all subscribers to a server group called “ADVT” for the initial 60 seconds of the session. After the initial 60 seconds, ISG will stop redirecting the traffic for the rest of the lifetime of the session.

```
service-policy type control initial-rdt
policy-map type control intial-rdt
 class type control always event session-start
  1 service-policy type service name initial-rdt-profile
 !
policy-map type service initial-rdt-profile
 class type traffic CLASS-ALL
  redirect to group ADVT duration 60
```

Example: Periodic ISG Redirection

The following example shows how to redirect all subscriber traffic for a period of 60 seconds every 3600 seconds:

```
service-policy control periodic-rdt session-start
!
policy-map type control periodic-rdt
 class type control always event session-start
  1 service-policy service periodic-rdt-profile
 !
policy-map type service periodic-rdt-profile
 redirect to group ADVT duration 60 frequency 3600
```

Example: Redirecting DNS Traffic

The following example shows how to redirect all subscriber DNS packets to the server group “DNS-server:”

```
service-policy type control DNS-rdt

policy-map type control DNS-rdt
 class type control event session-start
  1 service-policy type service name DNS-rdt-profile
  !
policy-map type service DNS-rdt-profile
 class type traffic CLASS-ALL
  redirect to group DNS-server
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Configuring ISG subscriber services	“Configuring ISG Subscriber Services?” module in this guide
HA commands	Cisco IOS High Availability Command Reference
HA configuration	*Cisco IOS High Availability Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Redirecting ISG Subscriber Traffic

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 135: Feature Information for Redirecting ISG Subscriber Traffic

Feature Name	Releases	Feature Information
ISG: Flow Control: Flow Redirect	Cisco IOS XE Release 2.2	The ISG Layer 4 Redirect feature enables service providers to better control the user experience by allowing subscriber TCP or UDP packets to be redirected to specified servers for appropriate handling. ISG Layer 4 redirection can be applied to individual subscriber sessions or flows.
Parameterization for ACL and Layer 4 Redirect	Cisco IOS XE Release 2.4	The Parameterization for ACL and Layer 4 Redirect feature provides parameterization enhancements for access control lists and Layer 4 redirect.
ISG: IPv6 Support phase II	Cisco IOS XE Release 3.5S	IPv6 support was added for the Layer 4 Redirect feature. The following commands were introduced or modified: **redirect session-limit**, **redirect to**, **server ip**, **show redirect group**, **show redirect translations**.
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for ISG features including the Layer 4 Redirect feature.

CHAPTER 102

Configuring Layer 4 Redirect Logging

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes the Layer 4 Redirect Logging feature.

Prerequisites for Layer 4 Redirect Logging

The Layer 4 Redirect feature must be enabled. For configuration information, see the module "Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" in the *Intelligent Services Gateway Configuration Guide, Cisco IOS XE*.

Information About Layer 4 Redirect Logging

ISG Layer 4 Redirect Logging

The Layer 4 Redirect Logging feature allows ISG to capture records of the creation and deletion events for Layer 4 redirect translation entries. These records can identify users who have applications that do not react to HTTP redirect.

The ISG router acts as an exporter of the Layer 4 redirect logging information, sending a UDP packet periodically to the configured external collector. The packet contains all of the Layer 4 redirect logging records, in the NetFlow version 9 export format, for IPv4, IPv6, and dual-stack sessions. The ISG router tracks every creation and deletion event for Layer 4 redirect translation entries on the router. A packet containing the logging records is generated and sent to the external collector after the first of one of the following events occurs:

- A predefined amount of Layer 4 redirect logging data has accumulated in the local buffer.

- A predefined amount of time has passed without the router sending any data records to the collector, and there are data records in the local buffer to be sent.

If more than one type of logging feature is configured on the same router (for example, network address translation (NAT) or Firewall), the number of events that can be generated at one time is shared among all of the logging features. Logging requests are served on a first-come first-serve basis.

Any external collector that supports the NetFlow version 9 or IP information export (IPFIX) protocol can be used to process Layer 4 redirect logging data exported by the ISG router.

Template Formats for Layer 4 Redirect Logging

The Layer 4 Redirect Logging records that the ISG router sends to the collector use a preconfigured template format. The NetFlow version 9 export packets include a NetFlow packet header followed by the data records and template records that define the structure of the data records, in a format corresponding to the configured template.

The following tables list the fields that are included in records sent to the external collector, in the basic and extended IPv4 and IPv6 templates. The fields are listed in the order in which they appear in the templates. All of the fields in the basic template are also included in the extended template. The last four fields listed in the tables below are the additional fields that are included only in the extended template.

Table 136: IPv4 Translation Entries Record in the Layer 4 Redirect Logging Template

Field Name	Field Type	Field Length (bytes)	Description
sourceIPv4Address	8	4	Source IPv4 address.
sourceTransportPort	7	2	Source port number in the transport header.
destinationIPv4Address	12	4	Destination IPv4 address.
destinationTransportPort	11	2	Destination port number in the transport header.
l4rServerIPv4Address	44000	4	Layer 4 redirect server IPv4 address.
l4rServerTransportPort	44001	2	Layer 4 redirect server port number.
protocolIdentifier	4	1	Protocol number in the IP header.
l4rEvent	44003	1	1—Translation Entry Create event 2—Translation Entry Delete event
l4rEventTimestamp	44004	4	Time stamp for this Layer 4 Redirect event.
inPackets	2	4	Incoming packet counter.
outPackets	24	4	Outgoing packet counter.
flowId	148	4	ASR internal identifier (EVSI#) of the session or traffic class on which the Layer 4 Redirect feature is configured.

Table 137: IPv6 Translation Entries Record in the Layer 4 Redirect Logging Template

Field Name	Field Type	Field Length (bytes)	Description
sourceIPv6Address	27	16	Source IPv6 address.
sourceTransportPort	7	2	Source port number in the transport header.
destinationIPv6Address	28	16	Destination IPv6 address.
destinationTransportPort	11	2	Destination port number in the transport header.
l4rServerIPv6Address	44002	16	Layer 4 redirect server IPv6 address.
l4rServerTransportPort	44001	2	Layer 4 redirect server port number.
protocolIdentifier	4	1	Protocol number in the IP header.
l4rEvent	44003	1	1—Translation Entry Create event 2—Translation Entry Delete event
l4rEventTimestamp	44004	4	Time stamp for this Layer 4 redirect event.
inPackets	2	4	Incoming packet counter.
outPackets	24	4	Outgoing packet counter.
flowId	148	4	ASR internal identifier (EVSI#) of the session or traffic class on which the L4R feature is configured.

How to Configure Layer 4 Redirect Logging

Enabling ISG Layer 4 Redirect Logging

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
5. **source** *interface-type interface-number*
6. **transport udp** *udp-port*
7. **export-protocol netflow-v9**
8. **template data timeout** *seconds*
9. **exit**
10. **redirect log translations** {**basic** | **extended**} **exporter** *exporter-name*

11. **exit**
12. **show flow exporter** *exporter-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**flow exporter** *exporter-name* **Example:** `Router(config)# flow exporter L4R-EXPORTER`	Creates the flow exporter and enters flow exporter configuration mode. • This command also allows you to modify an existing flow exporter.
Step 4	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `Router(config-flow-exporter)# destination 172.16.10.2`	Specifies the IP address or hostname of the destination system for the exporter.
Step 5	**source** *interface-type interface-number* **Example:** `Router(config-flow-exporter)# source gigabitethernet 0/0/0`	Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams.
Step 6	**transport udp** *udp-port* **Example:** `Router(config-flow-exporter)# transport udp 650`	Specifies the UDP port on which the destination system is listening for exported datagrams.
Step 7	**export-protocol netflow-v9** **Example:** `Router(config-flow-exporter)# export-protocol netflow-v9`	(Optional) Specifies the version of the NetFlow export protocol used by the exporter. • Default is **netflow-v9**.
Step 8	**template data timeout** *seconds* **Example:** `Router(config-flow-exporter)# template data timeout 120`	(Optional) Configure resending of templates based on a timeout.
Step 9	**exit** **Example:** `Router(config-flow-exporter)# exit`	Exits flow exporter configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 10	**redirect log translations** {**basic** | **extended**} **exporter** *exporter-name* **Example:** `Router(config)# redirect log translations basic exporter L4R-EXPORTER`	Enables the Layer 4 Redirect Logging feature for ISG. • For the*exporter-name* argument, enter the name of the exporter you configured in step 3.
Step 11	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 12	**show flow exporter** *exporter-name* **Example:** `Router# show flow exporter L4R-EXPORTER`	(Optional) Displays the current status of the specified flow exporter.

Configuration Examples for Layer 4 Redirect Logging

Example: Enabling Layer 4 Redirect Logging

The following example shows that a flow exporter named L4R-EXPORTER is enabled to send Layer 4 Redirect logging information to an external collector:

```
flow exporter L4R-EXPORTER
 destination 172.16.10.2
 source GigabitEthernet 0/0/0
 transport udp 650
 template data timeout 120
!
!
redirect log translations basic exporter L4R-EXPORTER
```

Example: Layer 4 Redirect Logging Events

Layer4 Redirect IPv4 Translation Entry Creation Event

```
Source IPv4 Address 10.1.1.1, Port 1024,
Destination IPv4 Address 10.10.1.1, Port 80,
L4R Server IPv4 Address 10.1.10.1, Port 8000,
Protocol TCP, Translation Entry Create Event
```

Layer 4 Redirect IPv6 Translation Entry Deletion Event

```
Source IPv6 Address 1000::1, Port 1024,
Destination IPv6 Address 2000::1, Port 80,
L4R Server IPv6 Address 2001:ABCD:14::6, Port 8000,
Protocol UDP, Translation Entry Delete Event
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Configuring Layer 4 redirect	"Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module in the *Intelligent Services Gateway Configuration Guide, Cisco IOS XE*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
NetFlow commands	Cisco IOS NetFlow Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Layer 4 Redirect Logging

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 138: Feature Information for Layer 4 Redirect Logging

Feature Name	Releases	Feature Information
Layer 4 Redirect Logging Enhancement	Cisco IOS XE Release 3.5S	Allows ISG to export Layer 4 redirect logging information to an external collector. The following command was introduced: **redirect log translations**.
RaBaPol Web Traffic L4 Redirect Logging Enhancement	Cisco IOS XE Release 3.5S	Allows ISG to export Layer 4 redirect logging information to an external collector.

CHAPTER 103

Configuring ISG Policies for Regulating Network Access

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports the use of policies for governing subscriber session bandwidth and network accessibility. This module provides information about the following methods of regulating session bandwidth and network access: Modular Quality of Service (QoS) command-line interface (CLI) policies and ISG policing.

Information About ISG Policies for Regulating Network Access

Methods of Regulating Network Access

ISG supports the following methods of regulating network access. Each of these methods can be applied to an ISG session and can be dynamically updated.

Modular QoS CLI (MQC) Policies

QoS policies configured using the MQC are supported for subscriber sessions only. MQC policies cannot be applied to ISG services.

ISG Policing

ISG policing supports policing of upstream and downstream traffic. ISG policing differs from policing configured using the MQC in that ISG policing can be configured in service profiles to support policing of traffic flows. MQC policies cannot be configured in service profiles. ISG policing can also be configured in user profiles and service profiles to support session policing.

Overview of ISG Policing

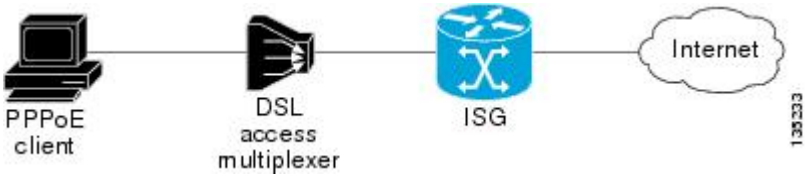
Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped or sent with a different priority.

ISG policing supports policing of upstream and downstream traffic and can be applied to a session or a flow. The following sections describe session-based policing and flow-based policing.

Session-Based Policing

Session-based policing applies to the aggregate of subscriber traffic for a session. In the figure below, session policing would be applied to all traffic moving from the PPPoE client to ISG and from ISG to the PPPoE client.

Figure 64: Session-Based Policing

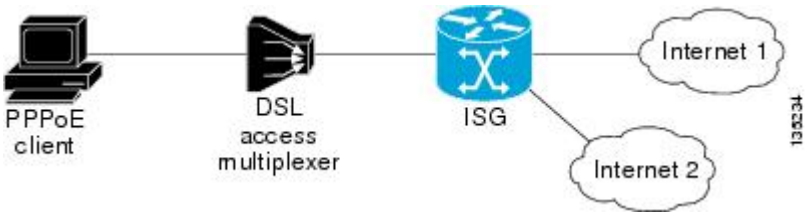


Session-based policing parameters can be configured on a AAA server in either a user profile or a service profile that does not specify a traffic class. It can also be configured on the router in a service policy map. Session-based policing parameters that are configured in a user profile take precedence over session-based policing parameters configured in a service profile or service policy map.

Flow-Based Policing

Flow-based policing applies only to the destination-based traffic flows that are specified by a traffic class. In the figure below, flow-based policing would allow you to police the traffic between the PPPoE client and Internet 1 or Internet 2.

Figure 65: Flow-Based Policing



Flow-based policing can be configured on a AAA server in a service profile that specifies a traffic class. It can also be configured on the router under a traffic class in a service policy map. Flow-based policing and session-based policing can coexist and operate simultaneously on subscriber traffic.

How to Configure ISG Policies for Regulating Network Access

Configuring ISG Policing

Configuring Policing in a Service Policy Map on the Router

Perform this task to configure ISG policing on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*]**class type traffic** *class-map-name*
5. **police input** *committed-rate normal-burst excess-burst*
6. **police output** *committed-rate normal-burst excess-burst*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service service1`	Creates or modifies a service policy map, which is used to define an ISG service.
Step 4	[*priority*]**class type traffic** *class-map-name* **Example:** `Router(config-service-policymap)# class type traffic silver`	Associates a previously configured traffic class with the policy map.
Step 5	**police input** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police input 20000 30000 60000`	Configures ISG policing of upstream traffic. • These parameters will be used to limit traffic flowing from the subscriber toward the network.

	Command or Action	Purpose
Step 6	**police output** *committed-rate normal-burst excess-burst* **Example:** `Router(config-service-policymap-class-traffic)# police output 21000 31500 63000`	Configures ISG policing of downstream traffic. • These parameters will be used to limit the traffic flowing from the network toward the subscriber.

What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Configuring Policing in a Service Profile or User Profile on the AAA Server

SUMMARY STEPS

1. Do one of the following:
   - Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server.
   - 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*"
   -
   - Add the following Policing VSA to the service profile on the AAA server.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Do one of the following: • Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server. • 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*" • • Add the following Policing VSA to the service profile on the AAA server. **Example:** `26,9,251 "QU;committed-rate;normal-burst;excess-burst;D;committed-rate;normal-burst;excess-burst"`	Enables ISG policing of upstream and downstream traffic. • If you specify the committed rate and normal burst, excess burst will be calculated automatically. • You can specify upstream or downstream parameters first.

What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

Verifying ISG Policing

Perform this task to verify ISG policing configuration.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier*	**uid** *session-id*| **username** *name*] **Example:** `Router# show subscriber session detailed`	Displays ISG subscriber session information.

Examples

The following example shows output for the **show subscriber session** command when policing parameters have been configured in the service profile. The “Config level” field indicates where the policing parameters are configured; in this case, in the service profile.

```
Router# show subscriber session detailed
Current Subscriber Information: Total sessions 2
Unique Session ID: 1
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Service
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service
.....
```

The following example shows output for the **show subscriber session** command where upstream policing parameters are specified in a user profile and downstream policing parameters are specified in a service profile.

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 2
Unique Session ID: 2
.....
```

```
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Per-user  ===========> Upstream parameters are specified in
the user profile.
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service ============> No downstream parameters in the user
profile, hence the parameters in the service profile are applied.
.....
```

Configuration Examples for ISG Policies for Regulating Network Access

ISG Policing Examples

Flow-Based Policing Configured in a Service Policy Map Using the CLI

The following example shows the configuration of ISG flow-based policing in a service policy map:

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203
policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

Session-Based Policing Configured in a User Profile on a AAA Server

The following example shows policing configured in a user profile:

```
Cisco:Account-Info = "QU;23465;8000;12000;D;64000"
```

Session-Based Policing Configured in a Service Profile on a AAA Server

The following example shows policing configured in a service profile:

```
Cisco:Service-Info = "QU;16000;D;31000"
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
How to configure QoS policies using the MQC	"Applying QoS Features Using MQC" module in the *Cisco IOS Quality of Service Configuration Guide*
How to configure DBS	"Controlling Subscriber Bandwidth" module in the *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for ISG Policies for Regulating Network Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 139: Feature Information for Policies for Regulating Network Access

Feature Name	Releases	Feature Configuration Information
ISG: Flow Control: QoS Control: Dynamic Rate Limiting	Cisco IOS XE Release 2.2	ISG can change the allowed bandwidth of a session or flow by dynamically applying rate-limiting policies.

CHAPTER 104

Configuring ISG Integration with SCE

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. This module describes how to configure ISG and Cisco Service Control Engine (SCE) to function as a single policy enforcement point for subscriber sessions.

Prerequisites for Configuring ISG Integration with SCE

Hardware Requirements

- An SCE platform
- Two connections between the ISG device and the SCE:
  - A control path, through which the ISG device and SCE can exchange policy information
  - A data path that carries the subscriber traffic
- A policy server configured to communicate with the ISG platform. The ISG-SCE integration removes any need for a communication layer between the policy server and the SCE.

Software Requirements

- Configure control and access policies, accounting, session maintenance, and network access regulation for ISG. For details on these configurations, see the *Cisco IOS Intelligent Services Gateway Configuration Guide.*
- Cisco Software Release 3.1.0 or later on the SCE

- Configure SCE appropriately. For instructions on configuring SCE, see the *Cisco Service Control Engine (SCE) Software Configuration Guide,* Release 3.1.

Restrictions for Configuring ISG Integration with SCE

The following restrictions apply to the integration of the ISG and an SCE:

- When an SCE policy is deactivated, the policy is removed from the session on the SCE, and the session policy reverts to the default SCE policy.
- Only one SCE policy at a time may be applied to a session. Applying additional policies will override the policy previously applied on the SCE.

This feature requires a control bus communication protocol, which runs over RADIUS and RADIUS extensions (as specified in RFC 3576), operating in two modes; PUSH and PULL.

- In PULL mode the ISG device waits for a query from the SCE.
- In PUSH mode the download of an external feature is initiated by the ISG device as soon as an external service is activated on the subscriber session.

To work with the SCE for subscriber management, the control bus protocol must do the following:

- Support pushing a session and make relevant changes to a session to the SCE.
- Allow a session, its relevant identity, and the SCE policy profile to be pulled from the ISG device by using an identity-based query.
- Support accounting events, including the following:
  - Accepting SCE initiated accounting events asynchronously.
  - Correlating SCE accounting data to the appropriate ISG session.
  - Parsing the SCE accounting data to perform protocol translation.

The per-user IP subnet assigned to Point-to-Point Protocol (PPP) users during login is not communicated to SCE. A per-user static route is downloaded to PPP users through the framed-route RADIUS attribute during login. ISG does not send the per-user subnet address for a PPP session to SCE in the CoA provision session (ProvSess) attribute.

Information About Configuring ISG Integration with SCE

Overview of ISG-SCE Integration

The ISG Integration with SCE feature integrates ISG and SCE at the policy plane level so that for purposes of subscriber provisioning, ISG and SCE function as a single logical entity. The ISG device and SCE communicate to manage subscriber sessions jointly, minimizing the requirements for coordination with additional external components. ISG handles subscriber management at Layer 4 and below. SCE is primarily focused at Layer 4 and above. When ISG and SCE are configured to work together, they provide tools for these functions:

- Subscriber mapping--Subscriber awareness is distributed between ISG and the SCE. The shared subscriber session is referenced by both devices using a unique session identifier allocated by the ISG. Identity keys such as IP Address, IP Subnet, network access server (NAS) identifier, and NAS port are also associated to the session. SCE policies that should be enabled on the session are identified by their policy names.
- Subscriber policy updates--Change subscriber policies in real time.

ISG and SCE Roles in Subscriber Management

The table below shows the specific roles of ISG and SCE in subscriber management.

Table 140: ISG and SCE Roles in Subscriber Management

Provided by ISG	Provided by SCE
Subscriber aggregation (broadband remote access service--BRAS) Subscriber authorization or authentication Policy management Policy enforcement for • Quality of service (QoS) • Multiprotocol label switching (MPLS) virtual private network (VPN) • Redirection • Session termination • Postpaid billing	Policy enforcement for • Application-aware services • Redirection and application-based policy management • Service security • Behavioral classification • URL caching and filtering • Value-added services • Parental controls • Usage and content billing

ISG pushes policies (or external services) to the SCE for a given subscriber session, in the form of RADIUS change of authorization (CoA) messages. External service activation can be triggered by the policy manager component inside the ISG or by an external authentication, authorization, and accounting (AAA) server. The SCE sees the ISG as the policy manager. ISG serves as a proxy for service activation requests from the external AAA server to the SCE. The SCE sends accounting records to the ISG. The ISG, if configured to do so, serves as a proxy that sends the accounting records to an external AAA server. SCE can also query the ISG about session information for unprovisioned sessions. ISG informs SCE when a session terminates by means of a RADIUS Packet of Disconnect (PoD).

How to Configure ISG Integration with SCE

Configuring Communication Between SCE and ISG

Communication between the SCE and the ISG device is managed by an external policy delegation (EPD) handler module in Cisco IOS software. The EPD implements the control bus on the ISG and handles all

messaging between the ISG device and SCE. This task is necessary to establish the parameters for the communication between the ISG device and the SCE, including the following:

- Port to which CoA messages are sent from the ISG device and SCE
- Port on which ISG should receive access, accounting, and connection management requests from SCE
- Shared secret between the ISG device and SCE

To configure communication between SCE and the ISG device, enter the following commands on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa server radius** {**sesm** | **proxy** | **policy-device**}
4. **client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret]*
5. **authentication port** *port-number*
6. **accounting port** *port-number*
7. **key** *shared-secret*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius** {**sesm** | **proxy** | **policy-device**} **Example:** `Router(config)# aaa server radius policy-device`	Enters RADIUS server configuration mode and configures the RADIUS profile.
Step 4	**client** *ipaddress* [**port** *coa destination port*] [**key** *shared secret]* **Example:** `Router(config-locsvr-radius)# client 10.10.10.1 key cisco port 1431`	Configures client-specific details. • The IP address identifies the destination for CoA messages. If no port is configured, the default port (3799) is used. ISG sends CoA messages to the SCE to provision, update, or deactivate a session and activate or deactivate policies.

	Command or Action	Purpose
		• A shared secret configured for a specific client overrides the key configured using the **key shared-secret**command.
Step 5	**authentication port** *port-number* **Example:** `Router(config-locsvr-radius)# authentication port 1433`	Specifies the port on which the EPD handler listens for session and identity query requests from SCE. • If no port is specified, the default port (1645) is used.
Step 6	**accounting port** *port-number* **Example:** `Router(config-locsvr-radius)# accounting port 1435`	Specifies the port on which the EPD handler listens for accounting and peering requests and maintenance packets from SCE. • If no port is specified, the default port (1646) is used.
Step 7	**key** *shared-secret* **Example:** `Router(config-locsvr-radius)# key xxxxxxxxxx`	Configures the secret shared between the EPD handler and SCE. • This key is used if no per-client shared secret is configured.
Step 8	**exit** **Example:** `Router(config-locsvr-rasius)# exit`	Exits RADIUS server configuration mode.

Configuring SCE Connection Parameter on ISG

To configure the server connection management on either a per-server or a global basis, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-peer address** *ip-address* **keepalive** *seconds*
4. **policy-peer keepalive** *seconds*
5. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-peer address** *ip-address* **keepalive** *seconds* **Example:** `Router(config)# policy-peer address 10.10.10.1 keepalive 6`	Configures the keepalive value, in seconds, for a specific policy defined by the given IP address. • Valid values are from 5 to 3600. • The default value is zero (0). • If the default value is in effect on the ISG device, the keepalive value proposed by the external policy device is used.
Step 4	**policy-peer keepalive** *seconds* **Example:** `Router(config)# policy-peer keepalive 10`	Configures the keepalive value, in seconds, globally. • The range of valid values is from 5 to 3600. • The default value is zero (0). • If no per-server keepalive value is configured, the global value is used. • If different values are configured on the ISG device and the SCE, the lower value is used as the keepalive interval. • If neither a per-server nor a global value is configured, the default value of zero is used.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Control Policy on the Policy Manager

To configure the policy manager to download a service, through rules configured by Cisco IOS commands, follow the steps in this section.

Configuring Control Policy on the ISG

To configure the control policy on the ISG device, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **policy-map type control** *policy-map-name*
4. **class type control** {*class-map-name* | **always**} **event session-start**
5. *action-number* **service-policy type service name** *service-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control GOLD_POLICY`	Configures the specified policy-map on the ISG and enters policy map configuration mode.
Step 4	**class type control** {*class-map-name* | **always**} **event session-start** **Example:** `Router(config-control-policymap)# class type control always event acct-notification`	Specifies to apply actions matching conditions defined by the class-map-name or always for an event type. • Event types include the following: account-logoff, account-logon, acct-notification, credit-exhausted, quota-depleted, service-failed, service-start, service-stop, session-default-service, session-restart, session-service-found, session-start, and timed-policy-expiry.
Step 5	*action-number* **service-policy type service name** *service-name* **Example:** `Router(config-control-policymap)# 1 service-policy type service name sce-service`	Defines the list of actions to be performed when the control policy is matched.
Step 6	**exit** **Example:** `Router(config-control-policymap)# exit`	Exits policy map configuration mode.

Configuring Auto Service on the AAA Server

To download a service to the ISG by means of auto service, perform the steps in this section.

SUMMARY STEPS

1. Cisco-Avpair="subscriber: auto-logon-service=sce-service"

DETAILED STEPS

Cisco-Avpair="subscriber: auto-logon-service=sce-service"

Downloads a service name from the SCE to the ISG device.

Configuring Services

To configure services, perform the steps in this section. You can configure this feature either on the ISG device, using the Cisco IOS command line interface (CLI) commands, or on the AAA server.

Configuring Services on ISG

To configure a service containing accounting features and to activate an external policy on the SCE device, follow the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *service-map-name*
4. **class-map type traffic** *class-map-name*
5. **accounting aaa list** *listname*
6. **sg-service-type external-policy**
7. **policy-name** *name*
8. **service-monitor enable**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**policy-map type service** *service-map-name* **Example:** `Router(config-traffic-classmap)# policy-map type service SVC`	Creates a service and enters traffic class map configuration mode.
Step 4	**class-map type traffic** *class-map-name* **Example:** `Router(config-control-policymap-class-control)# class-map type traffic bar`	Defines a traffic class and enters control policy-map class configuration mode.
Step 5	**accounting aaa list** *listname* **Example:** `Router(config-service-policymap)# accounting aaa list list1`	Configures accounting for ISG and enters service policy map configuration mode.
Step 6	**sg-service-type external-policy** **Example:** `Router(config-control-policymap)# sg-service-type external-policy`	Defines the service as an external policy and enters policy map configuration mode.
Step 7	**policy-name** *name* **Example:** `Router(config-control-policymap)# policy-name gold` **Example:**	Defines a corresponding external policy name on the SCE.
Step 8	**service-monitor enable** **Example:** `Router(config-control-policymap)# service-monitor enable` **Example:**	Enables service monitoring for the external policy device.
Step 9	**exit** **Example:** `Router(config-pol-map)# exit`	Exits policy map configuration mode.

Configuring Services on the AAA Server

To configure a service on the external AAA server, perform the steps in this section.

SUMMARY STEPS

1. Cisco:Avpair="subscriber:sg-service-type=external-policy"
2. Cisco:Avpair="subscriber:policy-name=gold"
3. Cisco:Avpair="subscriber:service-monitor=1"
4. Cisco:Avpair="accounting-list=list1"

DETAILED STEPS

Step 1 Cisco:Avpair="subscriber:sg-service-type=external-policy"

Defines the service as an external policy.

Step 2 Cisco:Avpair="subscriber:policy-name=gold"

Defines a corresponding external policy name on the ISG.

Step 3 Cisco:Avpair="subscriber:service-monitor=1"

Enables service monitoring for the external policy device.

Step 4 Cisco:Avpair="accounting-list=list1"

Configures accounting for ISG.

Troubleshooting Tips

The following command can be used to troubleshoot the integration of ISG with SCE:

- **show subscriber policy peer { address** *ip-address* **| handle** *connection-handle* **|** *id* **| all }**

Examples

This section contains sample output of the **show subscriber policy peer**command.

show subscriber policy peer all

The following example shows sample output of the command when the **all** keyword is used.

```
Router# show subscriber policy peer all
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:00:14
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:00:14
Remove owner on pull: TRUE
```

show subscriber policy peer all detail

The following example shows sample output for the **show subscriber policy peer**command when the **detail** keyword is added.

```
Router# show subscriber policy peer all detail
Peer IP: 10.0.0.10
Conn ID: 11
Mode   : PULL
State  : ACTIVE
Version: 1.0
Conn up time: 00:04:00
Conf keepalive: 0
Negotiated keepalive: 1000
Time since last keepalive: 00:04:00
Remove owner on pull: TRUE
Associated session details:
12.134.4.5session_guid_str
12.34.4.5session_guid_str
```

Configuration Examples for ISG Integration with SCE

ISG Control Bus Configuration Example

The following example shows how to configure the ISG control bus with the SCE management IP address and shared authentication key:

```
aaa server radius policy-device
 client 10.10.10.10
 key cisco
 message-authenticator ignore
!
policy-peer address 10.10.10.10 keepalive 60
!
interface GigabitEthernet5/1/1
 ip address 10.10.10.1 255.255.255.0
!
```

ISG Integration with SCE Example

The following example shows how to configure two SCEs, each with the same authentication and accounting ports. ISG handles CoA messages on port 1700 for one SCE and on default port 3799 for the other SCE. Peering is maintained for each SCE with the ISG via different keepalive intervals.

When a user session starts, POLICY-LOCAL is applied. If the user's profile at the AAA server has auto-logon, the session will begin using the SCE-SERVICE-LOCAL service. This service has the SCE service-monitor facility enabled. If the user profile does not specify auto-logon to the SCE-SERVICE-LOCAL service, SCE will use its default values for the *policy-name* argument and the **service-monitor**command, which are configured at the SCE.

```
aaa accounting network service_acct start-stop group radius
aaa accounting network session_acct start-stop group radius
aaa server radius policy-device
 authentication port 1343
```

```
 accounting port 1345
 message-authenticator ignore
 client 10.10.10.1 port 1341 key cisco
class-map type traffic match-any bar
 match access-group input 102
access-list 102 permit ip any any
policy-map type service sce_service
 class type traffic bar
  accounting aaa list service_acct
 sg-service-type external-policy
 policy-name gold
 service-monitor enable
policy-map type control sce_policy
 class type control always event session-start
   1 service-policy type service sce_service
 class type control always event acct-notification
  1 proxy aaa list session_acct
```

SCE Control Bus Configuration Examples

SCE Control Bus Setup Configured in PUSH Mode

The following example shows how to configure the SCE control bus in PUSH mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
scmp subscriber send-session-start
interface LineCard 0
 subscriber anonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

SCE Control Bus Setup Configured in PULL Mode

The following example shows how to configure the SCE control bus in PULL mode:

```
scmp
scmp name ISG radius 10.10.10.2 secret cisco auth 1433 acct 1435
interface LineCard 0
 subscriber anaonymous-group name all IP-range
  192.168.12.0:0xffffff00 scmp name ISG
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Intelligent Services Gateway Command Reference
AAA configuration tasks	The "Authentication, Authorization, and Accounting (AAA)" module in the*Cisco IOS Security Configuration Guide*
AAA commands	The "Authentication, Authorization, and Accounting (AAA)" module in the *Cisco IOS Security Command Reference*

Related Topic	Document Title
SCE configuration	*Cisco Service Control Engine (SCE) Software Configuration Guide*, Release 3.1

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Configuring ISG Integration with SCE

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 141: Feature Information for ISG Integration with SCE

Feature Name	Releases	Feature Information
ISG: Policy Control: ISG-SCE Control Bus	Cisco IOS XE Release 2.2	ISG accounting provides the means to bill for account or service usage. ISG accounting uses the RADIUS protocol to facilitate interaction between ISG and an external RADIUS-based AAA or mediation server. The following commands were introduced or modified: **aaa server radius policy-device**, **class type control**, **clear subscriber policy peer**, **clear subscriber policy peer session, policy-name**, **policy peer**, **proxy (ISG RADIUS proxy)**, **service-monitor**, **sg-service-type external policy**, **show subscriber policy peer**.

CHAPTER 105

Service Gateway Interface

The Service Gateway Interface (SGI) feature implements a web services interface to access the policy, subscriber, and session management functionality of the Intelligent Services Gateway (ISG). It allows application developers to author subscriber management applications using commonly available commercial and open source protocols, encoding, and toolkits.

ISG is a framework of components for the policy-based control of sessions and services on network devices. The SGI feature comprises the data model for policy and associated elements and the operational interface to provision, update, delete, and control activation of those policies.

Information About Service Gateway Interface

ISG

ISG is a Cisco IOS and Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. See "Overview of ISG" for further information.

BEEP

Block Extensible Exchange Protocol (BEEP) is a protocol standard that is scalable, efficient, simple, extensible, and robust. BEEP is a framework for designing application protocols.

Benefits of SGI

SGI is a protocol that allows Cisco IOS XE software to be controlled using third-party applications, toolkits, and development platforms for web services.

The SGI feature is a common model that can express ISG provisioning in many languages, and it is easy to use.

How to Enable Service Gateway Interface

Configuring BEEP Listener Connection

Perform this task to enable SGI.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sgi beep listener [** *port][* **acl** *access-list][* **sasl** *sasl-profile][* **encrypt** *trustpoint]*
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sgi beep listener [** *port][* **acl** *access-list][* **sasl** *sasl-profile][* **encrypt** *trustpoint]* **Example:** `Router(config)# sgi beep listener 2089`	Enables the SGI feature.
Step 4	end **Example:** `Router(config)# end`	Exits global configuration mode.

Troubleshooting SGI

Perform this task to troubleshoot the SGI.

SUMMARY STEPS

1. **enable**
2. **show sgi** [**session**| **statistics**]

3. **debug sgi** [**error**| **info**| **xml**| **gsi**| **isg-api**| **all**]
4. **test sgi xml** *filename*

DETAILED STEPS

Step 1 **enable**

Enables privilege EXEC mode. Enter your password if prompted.

Step 2 **show sgi** [**session**| **statistics**]

Displays information about current SGI session. This command shows information about SGI sessions that have been started and are currently running, including the running state. It also shows statistical information about SGI sessions that have been started and are currently running. The following is sample output from this command:

Example:

```
Router# show sgi session
sgi sessions: open 1(max 10, started 15
session id:1;started at 9:08:05; state OPEN

Router# show sgi statistics
sgi statistics
total messages received 45
current active messages 5; maximum active messages 7
total isg service requests 4
current active services 2; maximum active services 2
sgi process statistics
process sgi handler 1
pid 95, cpu percent (last minute) 1, cpu runtime 10(msec), memory accocated 4200 (bytes)
```

Step 3 **debug sgi** [**error**| **info**| **xml**| **gsi**| **isg-api**| **all**]

Enables debugging of SGI sessions. The following is sample output from this command when all debugging has been enabled:

Example:

```
Router# debug sgi all
Router# show debug

SGI:
SGI All debugging is on
SGI Errors debugging is on
SGI XML debugging is on
SGI Informational debugging is on
SGI Generic Service Interface debugging is on
SGI ISG_API Events debugging is on
SGI ISG_API Errors debugging is on
Router#
Router#
*Jul 1 20:55:11.364: SGI: Session created, session Id 7
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M number=1 answer=-1
 more=* size=1400
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: Content-Type: application/xml
<?xml version="1.0" encoding="UTF-8"?>
...
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: frame_available: type=M number=1 answer=-1
 more=. size=111
```

```
*Jul 1 20:55:11.372: sgi beep listen app beep[0x66245188]: gitypes:policyGroup>
</objects>
</sgiops:insertPolicyObjectsRequest>
...
*Jul 1 20:55:11.372: SGI: GSI message received, msgid 1, session 7
*Jul 1 20:55:11.376: SGI: XML parsed successfully, request insertPolicyObjectsRequest, msgid 1
*Jul 1 20:55:11.376: SGI: authentication request sent to AAA
*Jul 1 20:55:11.376: SGI: req = [0x67454088] authentication succeeded
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsRequest
*Jul 1 20:55:11.376: SGI: insertPolicyObjectsRequest processing policyGroup:VPDN1, type 1, result:
0
*Jul 1 20:55:11.376: SGI: Processing insertPolicyObjectsResponse
*Jul 1 20:55:11.376: SGI: GSI message sent, msgid 1, session 7
*Jul 1 20:55:12.088: sgi beep listen app beep[0x66245188]: close confirmation: status=+ no error
origin=L scope=C
*Jul 1 20:55:12.088: SGI: Session terminating, session Id 7
```

Step 4 **test sgi xml** *filename*

Verifies the format ofan SGI XML request. The XML file must be copied to the router before it can be used.

Configuration Examples for Service Gateway Interface

Configuring BEEP Listener Connection Example

The following example shows how to configure the BEEP listener connection. The port number is set to 2089.

```
enable
configure terminal
sgi beep listener 2089
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Overview of ISG	*Cisco IOS Intelligent Services Gateway Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• ~~a~~	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Service Gateway Interface

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 142: Feature Information for Service Gateway Interface

Feature Name	Releases	Feature Information
Service Gateway Interface	Cisco IOS XE Release 2.2	The SGI implements a web services interface to access the policy, subscriber, and session management functionality of ISG. The following commands were introduced or modified: **debug sgi**, **sgi beep listener**, **show sgi, test sgi xml**.

CHAPTER 106

ISG MIB

The Intelligent Services Gateway (ISG) MIB feature defines all objects relevant to subscriber session details, subscriber session statistics, and subscriber service information as MIB objects. These MIB objects are accessed using Simple Network Management Protocol (SNMP), and the network administrators can monitor their ISG box's session in a centralized management server for public wireless LAN deployment requirements.

Information About ISG MIB

ISG MIB Overview

The ISG MIB feature introduces MIB support in Cisco software. The ISG MIB is accessed using remote SNMP software clients. MIB table objects are accessed as read-only through GET, GETNEXT, GETBULK, SET, and TRAP (notification) requests.

Subscriber Session MIB

The CISCO-SUBSCRIBER-SESSION-MIB contains objects to monitor subscriber session details, session statistics, and job tables to query specific subscriber information.

The following tables are implemented from this MIB:

- Subscriber Session Table—This table contains detailed information about a subscriber session. Each row in the table represents a subscriber session. The table row (subscriber session) can be indexed through the ifIndex object, which is unique for each subscriber session.
- Subscriber Session Statistics Table—This table provides ISG box-wide subscriber session aggregate statistics information. Each subscriber's session statistics are accessed based on the scope of aggregation. Session type and entity are used to define the scope of aggregation.
- Subscriber Session Job Tables and Notification—These tables allow an Element Management System (EMS) or Network Management System (NMS) to submit a job to perform a query on a subset of the current subscriber sessions maintained by the ISG system. The EMS or NMS can create a job and provision it to perform an operation with specified parameters. Every query is a job for the ISG MIB and has a unique Job ID associated with it.

Dynamic Template MIB

The CISCO-DYNAMIC-TEMPLATE-MIB contains subscriber service information. This information is captured through Dynamic Template MIB definitions and presented in Object Identification (OID) format.

The following tables from the Dynamic Template MIB capture information about subscriber services, subscriber service association with sessions, and subscriber service usage:

- Template Table—This table stores basic subscriber service profile information. Each entry in the template table corresponds to a unique subscriber service. This table entry is uniquely identified with a service name.
- Template Association Table—This table is used to identify the list of subscriber services associated with each session.
- Template Usage Table—This table is used to identify the list of subscriber sessions using a particular subscriber service.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

MIBs

MIB	MIBs Link
• CISCO-DYNAMIC-TEMPLATE-MIB • CISCO-SUBSCRIBER-SESSION-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 143: Feature Information for ISG MIB

Feature Name	Releases	Feature Information
ISG MIB	Cisco IOS XE Release 3.7S	The Intelligent Services Gateway (ISG) MIB feature defines all objects relevant to subscriber session details, subscriber session statistics, and subscriber service information as MIB objects. These MIB objects are accessed using Simple Network Management Protocol (SNMP), and the network administrators can monitor their ISG box's session in a centralized management server for public wireless LAN deployment requirements.

CHAPTER 107

ISG SSO and ISSU

The SSO and ISSU feature for Intelligent Services Gateway (ISG) adds high availability (HA) support to ISG features.

Prerequisites for ISG SSO and ISSU

SSO and ISSU must be enabled on the ISG router. For configuration information, see the High Availability Configuration Guide, Cisco IOS XE Release 3S .

Information About ISG SSO and ISSU

High Availability for ISG Features

The SSO and ISSU feature provides high availability (HA) support for the following ISG features during a stateful switchover (SSO) or In Service Software Upgrade (ISSU) event:

Feature	Description	Configuration Information
Absolute timeout (session timer)	Timer is restarted on the new standby Route Processor (RP). During bulk synchronization to the standby RP, the remaining timeout duration is sent to the standby RP and used while the feature is being installed.	"Configuring ISG Policies for Session Maintenance" module in this guide
Idle timeout (connection timer)	Timer is restarted on the new standby RP.	"Configuring ISG Policies for Session Maintenance" module in this guide
ISG accounting	Cumulative counters and accounting ID are checkpointed to the standby RP.	"Configuring ISG Accounting" module in this guide

Feature	Description	Configuration Information
ISG policer (dynamic rate limiting)	HA support was enabled for this feature.	"Configuring MQC Support for IP Sessions" module in this guide
Keepalive	Associated timers are restarted after the control plane switchover.	"Configuring ISG Policies for Session Maintenance" module in this guide
Layer 4 redirect	Layer 4 redirect includes the selected service group in its checkpoint data during the initial session and bulk synchronization. The standby RP uses the service group instead of selecting a new one.	"Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module in this guide
Port-bundle host key (PBHK)	PBHK includes the allocated bundle ID in its checkpoint data during the initial session and bulk synchronization. Upon session replay, the standby RP reserves the bundle ID instead of allocating a new one.	"Configuring ISG Port-Bundle Host Key" module in this guide
Traffic classes	ISG traffic classes are checkpointed to the standby RP and established during session replay.	"Configuring ISG Subscriber Services" module in this guide

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
HA commands	Cisco IOS High Availability Command Reference
HA configuration	High Availability Configuration Guide, Cisco IOS XE Release 3S
Configuring ISG accounting	"Configuring ISG Accounting" module in this guide
Configuring ISG timers	"Configuring ISG Policies for Session Maintenance" module in this guide
Configuring Layer 4 redirect	"Redirecting Subscriber Traffic Using ISG Layer 4 Redirect" module in this guide

Related Topic	Document Title
Configuring port-bundle host key	"Configuring ISG Port-Bundle Host Key" module in this guide
Configuring traffic classes	"Configuring ISG Subscriber Services" module in this guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG SSO and ISSU

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 144: Feature Information for ISG SSO and ISSU

Feature Name	Releases	Feature Information
ISG: Flow Control: SSO/ISSU	Cisco IOS XE Release 3.5S	HA support was added for the following ISG features: • Absolute Timeout • Idle Timeout • ISG Accounting • ISG Policer • Keepalive • Layer 4 Redirect • Port-Bundle Host Key • Traffic Classes

CHAPTER 108

ISG Debuggability

The ISG Debuggability feature supports conditional debugging of simple IP subscriber sessions whereby debugs of only specified sessions appear in the debug log. The conditions that can be applied to the subscriber sessions include IP address, VRF (IPv4 or IPv6), and MAC address. This module describes how to enable conditional debuggability on Cisco Intelligent Services Gateway (ISG) subscriber sessions.

Restrictions for ISG Debuggability

- Conditional debugging is not available for service manager, QOS policy, most of the command handler, EPD controller, ANCP, and CCM. Also, L2TP, VPDN, PPP, and PPP-based sessions can not be conditionally debugged.

Information About ISG Debuggability

ISG Debugging Behavior

Prior to this enhancement, debugging could be enabled for individual modules through module-wise debugging commands. These debugs provide the flexibility to limit the debugs to a specified subset of modules. However, when these debugs were enabled to debug session-related issues, the logs contained debug information for all sessions which would sometimes be unmanageable depending on the scale. With the conditional debugging enhancement, the debug logs are limited to only specified sessions.

To determine if session debug logs are printed for the specified module, check the following conditions:

- Debug condition is configured for the session identifier
- Debug condition is enabled on the device
- Module debugging is enabled

Additional References for ISG Debuggability

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
ISG commands	ISG Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for ISG Debuggability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 145: Feature Information for ISG Debuggability

Feature Name	Releases	Feature Information
ISG Debuggability		The ISG Debuggability feature supports conditional debugging of simple IP subscriber sessions whereby debugs of only specified sessions appear in the debug log. The conditions that can be applied to the subscriber sessions include IP address, VRF (IPv4 or IPv6), and MAC address.. The following commands were introduced: **subscriber per-session debug**, **show subscriber log**, **show subscriber per-session debug sessions-hit**, **clear subscriber log**.

CHAPTER 109

Troubleshooting ISG with Session Monitoring and Distributed Conditional Debugging

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers.This document describes ISG session monitoring and distributed conditional debugging. Conditional debugging facilitates debug filtering for ISG and is available as distributed conditional debugging.

Prerequisites for ISG Session Monitoring and Distributed Conditional Debugging

Before using the information in this module, it is recommended that you be familiar with the use of Cisco IOS **debug** commands and conditional debugging. See the "Additional References" section to find information about these topics.

Restrictions for Distributed Conditional Debugging

Conditions that are set for an active session take effect only when the session is terminated and reestablished.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the Cisco IOS **debug**commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users, or on a debug chassis with a single active session. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Information About ISG Session Monitoring and Distributed Conditional Debugging

ISG Session and Flow Monitoring

ISG introduces a mechanism that allows an administrator to monitor ISG sessions and flows continuously. The **show interface monitor** command, which displays interface statistics, and the **show process cpu monitor** command, which displays information about CPU usage, both update the information in their displays at specified intervals. These commands also provide the ability to freeze or clear the information in the display.

ISG Distributed Conditional Debugging

Benefits of Enhanced Conditional Debugging for the ISG Platforms

Because thousands of user sessions run on the ISG platforms, it is not practical to troubleshoot a problem with a session by enabling the various component **debug** commands that are available and trace through the messages for a single session or user. Instead, it is more practical to filter debugging messages for a single session or call across the various Cisco IOS XE components that a session traverses. For this reason, the conditional debugging previously offered in the Cisco IOS XE software has been enhanced to facilitate debug filtering for ISG and is available as distributed conditional debugging.

Cisco IOS XE Software Components Supported by Distributed Conditional Debugging

The following components are supported for ISG distributed conditional debugging:

- Authentication, authorization, and accounting (AAA) and RADIUS
- Feature Manager
- Policy Manager
- PPP
- PPP over Ethernet (PPPoE)
- Session Manager
- Virtual Private Dialup Network (VPDN)

See Table 1 and Table 2 for specific commands that are supported for distributed conditional debugging.

How to Enable ISG Session Monitoring and Distributed Conditional Debugging

Monitoring ISG Sessions and Flows

Perform this task to monitor interface and CPU statistics. The **show** commands are not required and may be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show interface** *type number* **monitor** [**interval** *seconds*]
3. **show processes cpu monitor** [**interval** *seconds*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface** *type number* **monitor** [**interval** *seconds*] **Example:** `Router# show interface gigabitethernet 3/0/0 monitor interval 10`	Displays interface statistics that are updated at specified intervals.
Step 3	**show processes cpu monitor** [**interval** *seconds*] **Example:** `Router# show processes cpu monitor`	Displays detailed CPU utilization statistics that are updated at specified intervals.

Configuring Distributed Conditional Debugging

Two main tasks are required for configuring distributed conditional debugging: enabling conditional debugging, and issuing one or more supported **debug** commands. These required tasks are described in the following sections:

ISG Debug Condition Commands

The table below lists the **debug condition** commands that you can issue at the EXEC prompt to enable distributed conditional debugging. You can set more than one condition.

Table 146: Supported Conditional Debug Commands

Command	Purpose
debug condition domain *domain-name*	Filters messages on the specified domain name.
debug condition interface {**Fast Ethernet** | **Gigabit Ethernet** | **TenGigabit Ethernet**} **vlan-id** *ID*	Filters messages on the specified VLAN identifier.
debug condition mac-address *hexadecimal-MAC-address*	Filters messages on the specified MAC address.
debug condition portbundle ip *IP-address* **bundle** *bundle-number*	Filters messages on the specified Port-Bundle Host Key (PBHK).
debug condition session-id *session-ID*	Filters messages on the specified session identifier. **Note** The session identifier can be obtained by entering the **show subscriber session** command.
debug condition username *email-address*	Filters messages on the specified Internet username.

Debug Commands That Are Supported by ISG Conditional Debug

The table below lists the Cisco IOS debugging commands that are supported for distributed conditional debugging. The commands are listed by component. One or more of these commands can be issued after enabling one of the **debug condition** commands listed in the below table.

Table 147: Debug Commands Supported by ISG Distributed Conditional Debugging

AAA Debug Commands
debug aaa accounting
debug aaa authentication
debug aaa authorization
debug aaa id
PPP Debug Commands
debug ppp authentication
debug ppp bap error
debug ppp bap events
debug ppp bap negotiation
debug ppp cbcp
debug ppp error
debug ppp mppe detailed

AAA Debug Commands
debug ppp mppe events
debug ppp mppe pack
debug ppp multi data
debug ppp multi events
debug ppp multi frag
debug ppp negotiation
debug ppp pack
debug ppp subscriber
PPPoE Debug Commands
debug pppoe data
debug pppoe error
debug pppoe event
debug pppoe packet
Session Manager Debug Commands
debug subscriber aaa authorization event
debug subscriber aaa authorization fsm
debug subscriber error
debug subscriber event
Feature Manager Debug Commands
debug subscriber feature access-list error
debug subscriber feature access-list event
debug subscriber feature compression detail
debug subscriber feature compression error
debug subscriber feature compression event
debug subscriber feature detail
debug subscriber feature error
debug subscriber feature event
debug subscriber feature interface-config error

AAA Debug Commands
debug subscriber feature interface-config event
debug subscriber feature modem-on-hold detail
debug subscriber feature modem-on-hold error
debug subscriber feature modem-on-hold event
debug subscriber feature portbundle error
debug subscriber feature portbundle event
debug subscriber feature portbundle packet
debug subscriber feature qos-policy error
debug subscriber feature qos-policy event
debug subscriber feature static-routes error
debug subscriber feature static-routes event
debug subscriber feature traffic-classification detail
debug subscriber feature traffic-classification error
debug subscriber feature traffic-classification event
Policy Manager Debug Commands
debug subscriber fsm
debug subscriber policy condition
debug subscriber policy detail
debug subscriber policy error
debug subscriber policy event
debug subscriber policy fsm
debug subscriber policy rule
debug subscriber session error
debug subscriber session event
VPDN Debug Commands
debug vpdn call event
debug vpdn call fsm
debug vpdn error

AAA Debug Commands
debug vpdn event
debug vpdn event disconnect

Restrictions

The **debug condition session-id** command filters a session only after the session has been established. The session identifier is a unique dynamic number generated internally by the Cisco IOS software and assigned to each session when the session is established.

In VPDN, the **debug** commands and messages associated with tunnels cannot be filtered because they are not associated with a session, but are displayed during the tunnel-establishment phase. The debugging messages will be displayed even if filtering is enabled by one of the conditions.

If multiple conditions are set, the debugging messages corresponding to all the sessions that meet any of the conditions will be displayed. Some conditions, such as domain name, will trigger debugging messages for all the sessions that belong to the particular domain.

Enabling Distributed Conditional Debugging

Perform this task to enable distributed conditional debugging for ISG.

SUMMARY STEPS

1. **enable**
2. **debug condition** *command*
3. **debug** *command*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug condition** *command* **Example:** `Router# debug condition username user@cisco.com`	Enter one or more of the **debug condition** commands to enable distributed conditional debugging.
Step 3	**debug** *command* **Example:** `Router# debug subscriber aaa authorization fsm`	Enter one or more of the supported **debug** commands.

Displaying Debugging Conditions

To display the debugging conditions that have been set, perform the following task:

SUMMARY STEPS

1. **enable**
2. **show debug condition**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show debug condition** **Example:** `Router# show debug condition`	Displays conditions that have been set for debugging.

Troubleshooting Tips

The Cisco IOS software displays messages as you set the conditions for filtering the debugging.

When a condition is set, it is assigned a number, as follows:

```
Condition 1 set
```

If a condition has already been set, the following message is displayed:

```
% Condition already set
```

The following messages and prompt are displayed when you attempt to disable the last condition using the **no** form of a **debug condition** command:

```
This condition is the last interface condition set.
Removing all conditions may cause a flood of debugging messages
to result, unless specific debugging flags are first removed.
Proceed with removal? [yes/no]: yes
Condition 1 has been removed
```

Tip Use the **no** form of the commands to disable all **debug** commands before disabling all of the debugging conditions that have been set.

Configuration Examples for ISG Distributed Conditional Debugging

Monitoring Interface Statistics Example

The following example shows sample output for the **show interface monitor** command. The display will be updated every 10 seconds.

```
Router> show interface gigabitethernet 0/0/0 monitor interval 10
Router Name:  Scale3-Router8       Update Secs: 10
Interface Name:   GigabitEthernet 0/0/0 Interface Status: UP, line is up
Line Statistics:          Total:        Rate(/s)    Delta
Input Bytes:              123456        123         7890
Input Packets:              3456         56          560
Broadcast:                  1333          6           60
OutputBytes:               75717        123         1230
Output Packets:              733         44          440
Error Statistics:         Total:        Delta:
Input Errors:              0               0
CRC  Errors:               0               0
Frame Errors:              0               0
Ignored:                   0               0
Output Errors:             0               0
Collisions:                0               0
No. Interface Resets:  2
End = e       Clear = c      Freeze = f
```

Enter Command:

Monitoring CPU Statistics Example

The following example shows sample output for the **show processes cpu monitor** command:

```
Router> show processes cpu monitor

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs    5Sec   1Min     5Min    TTY Process
   3      772          712       1084    0.08%  0.04%    0.02%    0    Exec
  67      276         4151         66    0.08%  0.03%    0.01%    0 L2TP mgmt daemon
 116      604         2263        266    0.16%  0.05%    0.01%    0 IDMGR CORE

End = e    Freeze = f
```

Enter Command:

Enabling ISG Distributed Conditional Debugging Example

The following example shows how to filter PPP, PPPoE, and Session Manager debugs for a PPPoE session with username “user@cisco.com”. Only debugging messages for the defined user are displayed on the console. Any other debugging messages associated with other users will not be displayed.

```
Router# debug condition username user@cisco.com
```

```
Condition 1 set

Router# debug ppp negotiation
Router# debug pppoe event
Router# debug subscriber session event
```

Displaying Debugging Conditions Example

The following example shows how to display debugging conditions that have been set.

```
Router# show debug condition

Condition 1: domain cisco.com (0 flags triggered)
Condition 2: username user@cisco.com (0 flags triggered)
Condition 3: ip 172.19.200.10 (0 flags triggered)
```

Filtering Debug Output Example

In the following example, the output of the **debug subscriber packet detail** command is filtered on the basis of the username “cpe6_1@isp.com”:

```
Router# debug condition username cpe6_1@isp.com
Condition 1 set
Router# show debug

Condition 1: username cpe6_1@isp.com (0 flags triggered)

Router# debug subscriber packet detail
SSS packet detail debugging is on

Router# show debug
SSS:
  SSS packet detail debugging is on

Condition 1: username cpe6_1@isp.com (0 flags triggered)
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
Debug commands	*Cisco IOS Debug Command Reference*
Conditional debugging	"Conditionally Triggered Debugging" chapter in the *Cisco IOS Debug Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Distributed Conditional Debugging

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 148: Feature Information for ISG Session Monitoring and Distributed Conditional Debugging

Feature Name	Releases	Feature Configuration Information
ISG: Instrumentation: Session and Flow Monitoring	Cisco IOS XE Release 2.2	ISG provides a mechanism for continuously monitoring interface and CPU statistics. This feature introduces the **show interface monitor** and **show processes cpu monitor**commands, which display statistics that are updated at specified intervals.
ISG: Instrumentation: Advanced Conditional Debugging	Cisco IOS XE Release 2.2	ISG provides the ability to define various conditions for filtering debug output. Conditional debugging generates very specific and relevant information that can be used for session, flow, subscriber, and service diagnostics.

CHAPTER 110

Configuring ISG Troubleshooting Enhancements

The Intelligent Services Gateway (ISG) debugging enhancements enable you to more easily isolate issues with ISG subscriber sessions in a production network, such as a session getting stuck in a dangling state (never reaches the established state). The troubleshooting enhancements described in this module allow you to diagnose these issues by introducing expanded statistics collection and event tracing.

Information About ISG Troubleshooting Enhancements

Event Tracing for Subscriber Sessions

When trying to reproduce or capture customer issues, collecting debug output is not always practical or even possible. Network administrators often do not detect an error until long after the event that caused the error has occurred. By the time a fault is detected, it is usually too late to enable debug commands because the session is already in an error state, or the session was terminated because of an error.

Event tracing allows you to capture traces for existing sessions on the router and to retain the history of any past sessions that were marked as interesting, such as a session that became stuck in a dangling state. This enables you to look at existing sessions, as well as past sessions, and review the data after the session gets into an unexpected state or never comes up.

If a session is marked as interesting, its event trace information is sent to a history log, if history logging is enabled. A session is considered interesting if it becomes stuck in a state, enters an error state, or terminates without transitioning into a target state, because of a programming error, end-user action, packet drop, or other reason. The decision whether to log an event trace is determined by the after-the-fact status of the object. Event traces for uninteresting sessions are removed to free up space in the history log buffer.

Previously, the event trace data for each subscriber session was attached to its session context. This data was purged when the session was terminated. These enhancements preserve the event trace data even after the sessions are gone.

Each session context that supports event trace creates a new event trace log to hold the event traces for that session context. The event trace logs can be displayed independently through **show** commands.

Dumping Event Traces

ISG event traces are enabled to capture the trace logs by default. All the event trace logs are stored in the device memory. When the device reloads due to crash, the trace logs are lost and it becomes difficult to debug issues that causes the crash.

To prevent losing the trace logs, event trace logs are saved in a pre-configured file. ISG event traces are collected and saved in a file that is pre-configured in the device. If the filename is not configured, event traces cannot be collected. So, it is recommended to configure the filename to collect and save event trace logs during a crash.

Note To collect the event traces, ensure to configure the file location as bootflash. You cannot collect the event traces in a hard disk.

This example shows how to collect the event traces in a text file.

```
Device #
Device # configure terminal
Device(config)# monitor event-trace subscriber dump-file bootflash:isg_dump_file.txt
```

How to Enable ISG Troubleshooting Enhancements

Enabling Event Tracing for ISG Sessions

Perform the following steps to enable event tracing for ISG subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor event-trace subscriber** *dump-file*
4. **monitor event-trace subscriber enable**
5. **exit**
6. **no monitor event-trace subscriber**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**monitor event-trace subscriber** *dump-file* **Example:** `Router(config)# monitor event-trace subscriber dump-file`	Sets the dump file name to be used to collect traces.

Step 4	**monitor event-trace subscriber enable**
	Example:
	`Router(config)# monitor event-trace subscriber enable`
	`Router(config)# monitor event-trace subscriber ?`
	`feature Feature manager traces`
	`gx GX traces`
	`ip-sip IP-SIP traces`
	`policy Policy manager trace`
	`ppp PPP traces`
	`service Service manager trace`
	`session Subscriber Subsystem trace`
	`vpdn VPDN Traces`
		Enables event tracing for all the subscriber sessions.
		Note You can enable event tracing for ISG componets, IP-SIP, policy, PPP, service, session, VPDN, and feature.

Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**no monitor event-trace subscriber** **Example:** `Router(config)# no monitor event-trace subscriber`	Disables traces for all components at all levels.

Displaying Event Traces for ISG Sessions

Use the following commands to display information about the event traces that are saved in text file.

SUMMARY STEPS

1. **show monitor event-trace subscriber**

DETAILED STEPS

show monitor event-trace subscriber

Use this command to display about the event traces that were saved in text file.

Example:

```
Router# show monitor event-trace subscriber
all-traces Show all the event traces
 feature Feature manager trace
 gx GX trace
 identifier Filter traces based on identity of session
 ip-sip IP-SIP trace
 policy SSS Policy manager trace
 ppp PPP trace
 service Service manager trace
 session SSS trace
 vpdn VPDN trace
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Debug commands	Cisco IOS Debug Command Reference .
DHCP Configuration	Part 3, “DHCP,” *IP Addressing Configuration Guide*.
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
ISG subscriber sessions	"Configuring ISG Access for IP Subscriber Sessions" module in this guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for ISG Troubleshooting Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 149: Feature Information for ISG Troubleshooting Enhancements

Feature Name	Releases	Feature Information
Dumping event-traces along with the crash	Cisco IOS XE Fuji 16.9.1	ISG event traces are enabled to track trace logs. The following command is introduced. **monitor event-trace subscriber** *dump-file bootflash:isg_dump_file.txt*

CHAPTER 111

Gx Diameter Support for ISG sessions

This chapter describes the Gx Diameter Support for Intelligent Services Gateway (ISG) sessions. This feature supports the Gx Diameter interface and the Diameter 3GPP Application Gx interface. The component that initiates the Gx communication is through the Intelligent Services Gateway (ISG). Diameter provides a base protocol that can be extended in order to provide authentication, authorization, and accounting (AAA) services to new access technologies.

Restrictions for Gx Diameter Support for ISG Sessions

- GX Interface is supported only for IPoE Sessions
- Dynamic policy construction is restricted only for Dynamic Rate Limiting (DRL) and Differentiated Services Code Point (DSCP).
- ISG policies with the same name and different definitions are not supported.
- Gx Diameter in combination with radius is not supported.
- Subscription-ID Grouped AVP is shared only in credit-control messages.

The following base protocol features are not supported in ISG with Diameter:

- Communication with diameter peers that act as proxy, relay or a redirection agent
- Diameter peer discovery
- SCTP as the transport protocol for Diameter messages
- Internet Protocol Security (IPSec)

Information About Gx Diameter Support for ISG Sessions

Overview of the Diameter Protocol

Diameter is a peer-to-peer protocol that consists of a base protocol and a set of applications that allows it to extend its services to provide authentication, authorization, and accounting (AAA) services to new access technologies. The base protocol provides basic mechanisms for reliable transport, message delivery, and error handling and the base protocol must be used in conjunction with a Diameter application. Each application relies on the services of the base protocol to support a specific type of network access. Each application is defined by an application identifier and associated with commands. Each command is defined with mandatory Attribute Value Pairs (AVPs) and non-mandatory AVPs including vendor-specific AVPs.

Diameter allows peers to exchange a variety of messages. The Diameter client generates Diameter messages to the Diameter server to perform the AAA actions for the user. This protocol also supports server-initiated messages, such as a request to cancel the service to a particular user.

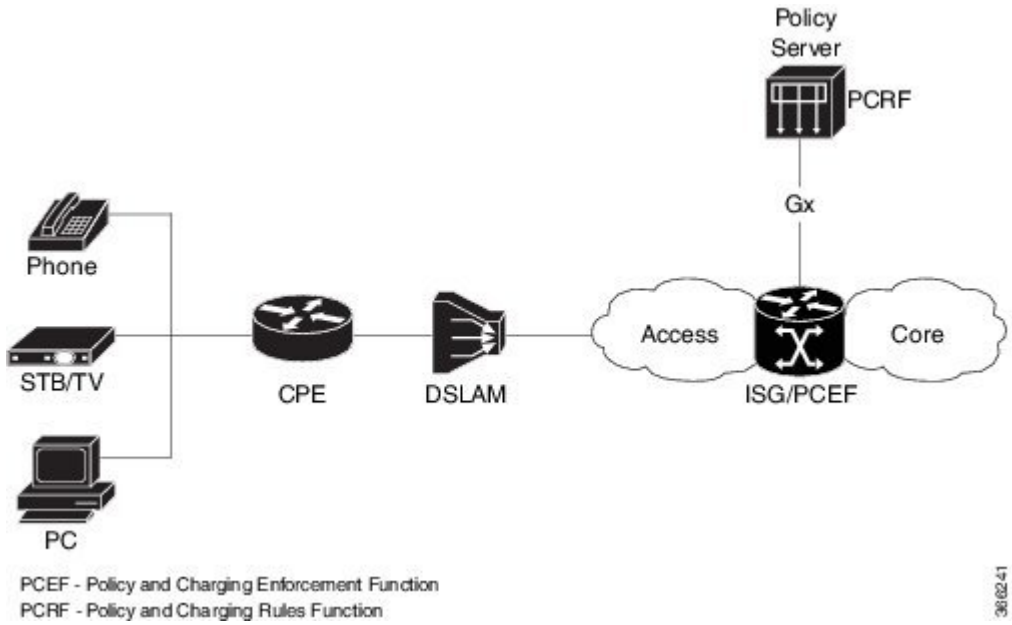
Gx Diameter Interface in ISG

The Gx Interface is located between the Policy and Charging Enforcement function (PCEF) and the Policy and Charging Rules Function (PCRF). Gx reference point is used to provision, modify and remove rules for policy and charging control from the PCRF to the PCEF. The policies downloaded are installed on the ISG session and any monitoring events installed is detected and notified to PCRF.

ISG Supports the download of policy information from radius server and the same is extended to integrate with GX interface for the PCEF functionality.

The following figure shows the network of the Diameter interface in ISG:

Figure 66: Diameter Interface in ISG



Along with the Diameter base protocol, the following Diameter applications are also supported in ISG:

- Diameter Credit Control Application (DCCA)
- Gx interface for Policy Control and Charging

The following table lists Internet Assigned Numbers Authority (IANA)-assigned application IDs for Diameter applications:

Diameter Application	Diameter Application ID
Diameter common message	0x00000000
Diameter policy interface(Gx)	0x01000016 (16777238)

Features supported for ISG with Diameter

These base protocol features are supported in ISG with Diameter:

- Transmission Control Protocol (TCP) as the transport protocol for Diameter messages
- Transport Layer Security (TLS) support over TCP for secure communication
- IPv4 transport stack to the back end Diameter server

Diameter Credit Control Application Application

Diameter Credit-Control Application (DCCA) interface implementation is based on the RFC 4006. The Diameter Gx application handles Gx messages and AVPs specific to Gx and DCCA application to provide support for the PCEF functionality. The DCCA messages supported on the Intelligent Services Gateway(ISG) are:

ISG supports these DCCA messages:

- Credit Control Request (CCR)
- Credit Control Answer (CCA)
- Re-Auth-Request (RAR)
- Re-Auth-Answer (RAA)

Every single CCR must be responded with a separate CCA.

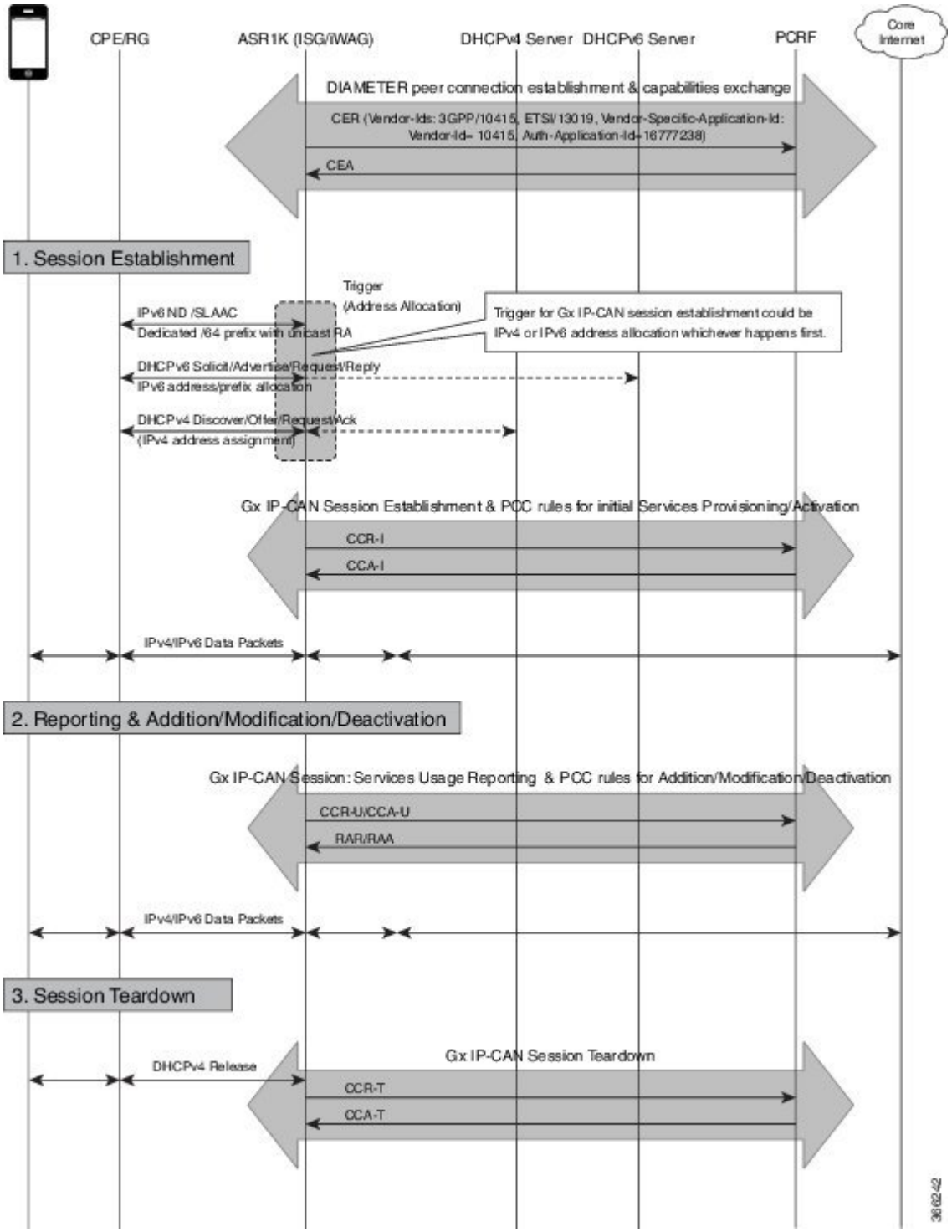
DCCA Session and Services

Each ISG subscriber session is associated with a Diameter IPCAN-session when Gx is enabled. The device implements the state machine for an IPCAN-session as per RFC-4006.

A Diameter session-id uniquely identifies an IPCAN-session.

ISG Diameter Call Flow

The following figure shows a call flow sequence of Gx Diameter:



Supported AVPs for Gx Diameter on ISG

The following table lists the AVPs supported for Gx Diamter on ISG.

AVP			CCR	CCA	RAR	RAA	Description
ID	Name	Type					
8	Framed-IP-Address	OctetString	0-1	0	0	0-1	
97	Framed-IPv6-Prefix	OctetString	0-1	0	0	0-1	
258	Auth-Application-Id	Unsigned32	1	1	1	0	3GPP Gx (16777238)
263	Session-Id	UTF8String	1	1	1	1	
264	Origin-Host	DiameterIdentity	1	1	1	1	
268	Result-Code	Unsigned32	0	1	0	0-1	
279	Failed-AVP	Grouped	0-1	0-n	0	0-1	
281	Error-Message	UTF8String	0	0-1	0	0-1	
283	Destination-Realm	DiameterIdentity	1	0	1	0	
285	Re-Auth-Request-Type	Enumerated	0	0	1	0	
293	Destination-Host	DiameterIdentity	0-1	0	1	0	
295	Termination-Cause	enumerated	0-1	0	0	0	
296	Origin-Realm	DiameterIdentity	1	1	1	1	
297	Experimental-Result	Grouped	0	0-1	0	0-1	
298	• Experimental-Result-Code	Unsigned32	0	n	0	n	
415	CC-Request-Number	Unsigned32	1	1	0	0	
416	CC-Request-Type	Enumerated	1	1	0	0	
443	Subscription-Id	Grouped	0-1	0	0	0	
450	• Subscription-Id-Type • Subscription-Id-Data	Enumerated	0-1	0	0	0	END_USER_NAI (3), END_USER_PRIVATE (4)
444		UTF8String	0-1	0	0	0	user-name@domain, NAS-Port-ID

AVP			CCR	CCA	RAR	RAA	Description
ID	Name	Type					
1001	Charging-Rule-Install • Charging-Rule-Name • Charging-Rule-Definition • Precedence • Flow-Information • Packet-Filter-Identifier • Flow-Direction • QoS-Information • Qos-Class-Identifier • -Max-Requested-Bandwidth-DL • -Max-Requested-Bandwidth-UL	Grouped	0	0-n	0-n	0	
1005		OctetString	0	1	1	0	
1003		Grouped	0	0-1	0-1	0	
1010		Unsigned32	0	1	1	0	
1058		Grouped	0	0-2	0-2	0	
1060		OctetString	0	1-n	1-n	0	
1080		Enumerated	0	1	1	0	
1016		Grouped	0	0-1	0-1	0	
1028		Enumerated	0	0-1	0-1	0	
515		Unsigned32	0	0-1	0-1	0	
516		Unsigned32	0	0-1	0-1	0	
1002	Charging-Rule-Remove • Charging-Rule-Name • Charging-Rule-Base-Name	Grouped	0	0-n	0-n	0	
1004		UTF8String	0	1	1	0	
1005		OctetString	0	1	1	0	
1027	IP-CAN-Type	Enumerated	0-1	0	0	0-1	Non-3GPP-EPS (6) for WiFI & FBA (7) for xDSL, FTTx
1018	Charging-Rule-Report • PCC-Rule-Status • Rule-Failure-Code	Grouped	0-1	0	0	0-1	
1019		Enumerated	0-1	0	0	0-1	
1031		Enumerated	0-1	0	0	0-1	
1045	Session-Release-Cause	Enumerated	0-1	0	0-1	0	
266	Vendor-ID	Unsigned32	0	1	0	1	
1066	Monitoring-Key	OctetString	0	1	1	0	
431	Granted-Service-Unit	Grouped	0	1	1	0	
420	CC-Time	Unsigned32	1	1	1	1	
421	CC-Total-Octets	Unsigned64	1	1	1	1	

AVP			CCR	CCA	RAR	RAA	Description
ID	Name	Type					
412	CC-Input-Octets	Unsigned64	1	1	1	1	
414	CC-Output-Octets	Unsigned64	1	1	1	1	
446	Used-Service-Unit	Grouped	1	0	0	1	
1067	Usage-Monitoring-Information	Grouped	1	1	1	1	
1068	Usage-Monitoring-Level	Enumerated	0	1	1	0	
1069	Usage-Monitoring-Report	Enumerated	0	1	1	0	
1070	Usage-Monitoring-Support	Enumerated	0	1	1	0	
1006	Event-Trigger	Enumerated	1	0	1	0	

RADIUS Server Configuration

Following AVPs for Cisco IOS XE Release 16.7.1 are enabled through RADIUS server configuration. Use **radius-server** command for the configuration.

How to Configure Gx Diameter Support on ISG Sessions

Configuring Diameter peer in ISG

Perform this task to configure the Diameter connection on a ISG router.

The selection of Diameter server is mostly based on the AAA method list configuration.

```
diameter timer watchdog 300
diameter origin realm cisco.com
diameter origin host 10.0.0.1
diameter source interface gigabitethernet 0/0/0
diameter vendor supported 3gpp
diameter vendor app gx
diameter peer PCRF
    address ipv4 10.0.0.2
    transport tcp port port1
    source interface Ethernet0/0
```

Configuring AAA for Diameter Peer in ISG

Perform this task to configure AAA for diameter server group. Prior to this task, you must set up the Diameter peer in ISG device.

```
aaa group server diameter GX_SG
server name PCRF
```

```
aaa authorization policy-if policy_meth group GX_SG
aaa authorization subscriber-service default local
```

Configuring Diameter Interaction for ISG

Note The method-list used aaa configuration and diameter interation configuration must be the same. The control policy should trigger gx session in both session-start and session-restart. In case of session-start, it is recommended to configure **collect identifier source-ip-address** before authorization

Peform the following task to configure Diameter interaction for ISG:

```
policy-map type control GX_TEST
    class type control always event session-start
        5 collect identifier source-ip-address
        10 authorize aaa list policy_meth identifier nas-port
    class type control always event session-restart
        10 authorize aaa list policy_meth identifier nas-port
```

Verifying the Gx Diameter Support for ISG Sessions

The following sample output is from the **show diameter gx session all** command.

```
Device#show diameter gx session all

Current Gx Sessions
ClientID     Session State     Subscription Data            IPCAN Sess ID
115425         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115425;1488824608
115430         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115430;1488824608
115432         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115432;1488824608
115434         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115434;1488824608
115436         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115436;1488824608
115442         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115442;1488824608
115444         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115444;1488824608
115447         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115447;1488824608
115449         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115449;1488824608
115451         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115451;1488824608
115453         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115453;1488824608
115455         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115455;1488824608
115457         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115457;1488824608
115459         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115459;1488824608
115461         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115461;1488824608
115463         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115463;1488824608
115465         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115465;1488824608
115467         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115467;1488824608
115469         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115469;1488824608
115471         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115471;1488824608
115473         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115473;1488824608
115475         OPEN              nas-port:0.0.0.0:0/3/3       device1;0;115475;1488824608
```

The following sample output is from the **show diameter gx session id** command.

```
Device# show diameter gx session id device1;0;4120;1488910407
```

```
Current Gx Sessions
ClientID     Session State     Subscription Data            IPCAN Sess ID
4120    OPEN               nas-port:0.0.0.0:255/0/8/10        device1;0;4120;1488910407
```

The following sample output is from the **show diameter gx statistics** command.

```
Device#show diameter gx statistics

CCR Initial messages                            : 295110
CCR Initial messages sent failed                : 21567
CCR Initial messages timed out                  : 184526
CCR Initial messages retry                      : 165003

CCR Update messages                             : 117667
CCR Update messag sent Failed                   : 0
CCR Update messages timed Out                   : 20828
CCR Update messages retry                       : 20418

CCR Terminate messages                          : 150241
CCR Terminate messages sent failed              : 149331

CCA Initial messages                            : 159270
CCA Initial messages error                      : 0
CCA Initial messages protocol error             : 0
CCA Update messages                             : 109513
CCA Update messages error                       : 2
CCA Update messages protocol error              : 0
CCA Terminate messages                          : 67679
CCA Terminate messages error                    : 0
CCA Terminate messages protocol error           : 0

RAR received messages                           : 0
RAR received messages error                     : 0
RAA sent messages                               : 0
RAA sent messages Error                         : 0

DIAMETER End User Service Denied                : 0
DIAMETER Credit Control Not Applicable          : 0
DIAMETER Credit Limit Reached                   : 0
DIAMETER Unknown Session Id                     : 0
DIAMETER Authorization Rejected                 : 0
DIAMETER Invalid AVP Value                      : 0
DIAMETER User Unknown                           : 0

Number of sessions currently up                 : 9308
Number of sessions closed                       : 141268
Highest number of sessions ever up at one time  : 159270
Number of sessions failed to come up            : 157407
Number of Unknown request messages              : 0
```

Examples: Configuring Gx Diameter Support for ISG Sessions

The following example shows the AVP representation of pre-defined policy.

```
Policy-Install
Charging-Rule-Install
    Charging-Rule-Name = TC_SERVICE1
```

```
    Charging-Rule-Name = ISG_L4R_SRV

Policy-Remove
Charging-Rule-Remove
    Charging-Rule-Name = TC_SERVICE2
    Charging-Rule-Name = TC_SERVICE1

Install and Remove
Charging-Rule-Insall
   Charging-Rule-Name = TC_SERVICE2
Charging-Rule-Remove
   Charging-Rule-Name = ISG_L4R_SRV
```

The following example shows the ISG-TC service representation of pre-defined policy.

```
policy-map type service TC_SERVICE1
    class type traffic VLAN_EFv4
        accounting aaa list EF_acct
        police input 300000
        police output 300000
    !
policy-map type service TC_SERVICE2
    class type traffic VLAN_EF
        accounting aaa list EF_acct
        police input 300000
        police output 300000
  !
Policy-map type service ISG_L4R_SRV
    Class type traffic class1
        Redirect to ip 10.10.10.10
```

The following example shows the AVP representation of static and dynamic policy.

```
Charging-Rule-Install
    Charging-Rule-Name = TC_SERVICE1

   Charging-Rule-Definition
      Charging-Rule-Name = TC_SERVICE2
      Flow-Information
         Flow-Direction = UPLINK
        Packet-Filter-Identifier = CS1_V6
      Qos-Information
         Max-Requested-Bandwidth-UL = 50000
```

The following example shows ISG-TC service for static and dynamic policy.

```
policy-map type service TC_SERVICE1
    class type traffic VLAN_EFv4
        police input 300000
        police output 300000
!
policy-map type service TC_SERVICE2
   class type traffic VLAN_CS1_V6
      police input 50000
!
class-type traffic match-any VLAN_CS1_V6
   match access-group input name CS1_V6
!
ipv6 access-list CS1_V6
```

```
permit ipv6 any any dscp cs1
```

Additional References

Related Documents

Related Topic	Document Title
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Finding Feature Information for Gx Diameter Support for ISG Sessions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 150: Feature Information for Gx Diameter Support for ISG Sessions

Feature Name	Releases	Feature Configuration Information
Gx Diameter Support for ISG Sessions	Cisco IOS XE Everest 16.5.1b	Diameter provides a base protocol that can be extended in order to provide authentication, authorization, and accounting (AAA) services to new access technologies. This chapter provides information about Diameter protocol and its support in ISG. The following command was introduced by this feature: **diameter timer watchdog** , **diameter origin realm** , **diameter origin host** , **diameter source interface** , **diameter vendor supported** , **diameter peer**,**show diameter gx session all**, **show diameter gx session id**, **show diameter gx statistics**

CHAPTER 112

Gx Diameter Monitoring and Reporting

This module describes how to configure an Internet Service Provider to monitor the data utilized by subscribers and enforce restrictions on the amount of data utilized and bandwidth consumed. This feature runs on a repeated authorization model and helps enforce quota restrictions on the volume of traffic flows in the iEdge architecture framework. Monitoring and reporting can be requested by the PCRF (Policy Control Rules Function) with a CCA (Credit Control Answer) or RAR (Re-Authorization Request) message for an individual PCC (Policy Control and Charging) rule or for all rules activated during a subscriber session

Prerequisites for Gx Diameter Monitoring and Reporting

- Rule based monitoring must be installed at the time of rule installation
- The user must have knowledge of configuring Diameter applications

Restrictions for Gx Diameter Monitoring and Reporting

- GX Interface is supported only for IPoE Sessions
- Cisco IOS XR Everest 16.6.1 release supports monitoring of traffic flows based on the volume of data consumed. Monitoring of traffic flows based on the time utilized for a session is not supported in this release.
- This features works by reporting accumulated usage based on last reported data using a CCR message. If PCRF updates the quota before actual exhaustion of quota, ISG triggers a CCR-U (Credit Control Request- Update) immediately if the newly downloaded slice of quota has already exceeded the limit.

- It is not possible to use the same Monitoring-Key charging rule definition for session-level and rule-level configuration.
- Modification of session-level monitoring key is possible only after disabling the existing monitoring instance

Information About Gx Diameter Monitoring and Reporting

Overview of Usage and Report Monitoring

This module describes how to configure an Internet Service Provider to monitor the data traffic utilized by subscribers and enforce restrictions on the amount of data utilized and bandwidth consumed. This feature runs on a repeated authorization model and helps enforce quota restrictions on the volume of traffic flows in the iEdge architecture framework. Monitoring and reporting can be requested by the PCRF (Policy Control Rules Function) with a CCA (Credit Control Answer) or RAR (Re-Authorization Request) message for an individual PCC (Policy Control and Charging) rule or all rules activated during a session.

The counters (octets/bytes) consumed by a subscriber in Subscriber Gateway (ISG) are monitored and reported back to the Diameter server. The monitoring criteria is defined and controlled by the Diameter server. You can use Monitoring-Key and Granted-Service-Unit AVP (Attribute Value Pair) to monitor all the sessions for a subscriber or monitor specific traffic flows in a subscriber session. By monitoring specific traffic flows, you can either exclude traffic for a specific session or monitor a combination of one or more traffic flows for a session

The ISG triggers monitoring of usage in the following scenarios:

- The downloaded prepaid quota is exhausted
- A RAR message is sent by PCRF
- All the services associated with the Monitoring-Key charging rule definition are removed
- When the subscriber session is terminated
- Monitoring is specifically disabled by PCRF by setting Usage-Monitoring-Support AVP to USAGE_MONITORING_DISABLED

The ISG keeps track of the volume usage from the moment monitoring is enabled and resets the counters after reporting the existing usage. For example, if the user is allocated 500 MB, 200 MB is downloaded at start of the session. After reporting that 200 MB is consumed, the counter is reset to zero.

Benefits

- Provides the flexibility to monitor prepaid or postpaid traffic flows. This flexibility of configuration allows you to cover monitoring and reporting for varied customer needs
- Configure rules to monitor all the traffic of a subscriber session or monitor specific traffic flows in a subscriber session. You can also configure a combination of rules that will help you monitor varied usage patterns of the subscribe
- Utilize predefined ISG redirection policies to redirect the user to a portal where the user can replenish the quota without being disconnected from the service.

Types of Reporting and Monitoring

The Monitoring and Reporting feature is supported in two models:

- **Prepaid** - In this scenario, information about quota allocated is sent to ISG. Monitoring and reporting is based on this quota. Monitoring of prepaid quota can be performed in the following scenarios:
  - Prepaid at Session Level - Quota is allocated for an entire subscriber session.
  - Prepaid at Flow Level - Quota is allocated for only a specific traffic flow in a subscriber session.
  - Prepaid at Session Level excluding some flows - Quota is allocated for an entire subscriber session except for a specific traffic flow in a session.
  - Prepaid at Flow Level with multiple flows - Quota is allocated for multiple traffic flows in a subscriber session.

  In all prepaid scenarios, the information in Granted-Service-Unit AVP is included in the Usage-Monitoring-Information AVP. Monitoring and reporting of prepaid quota automatically occur on the following triggers:
  - The subscriber session ends.
  - All the rules associated with the Monitoring-Key charging rule definition are removed.
  - A RAR message is sent to PCRF
  - The accumulated counters exceed the prepaid quota allocated

  Monitoring by PCRF can be disabled by setting Usage-Monitoring-Support AVP to USAGE_MONITORING_DISABLED.

- **Postpaid** - In this scenario no quota is provided, but data usage is monitored and reported to PCRF, when queried. Monitoring of postpaid can be performed in the following scenarios:
  - Postpaid at Session Level - Monitoring is done for a subscriber session.
  - Post-Paid at Flow Level - Monitoring is done for a specific traffic flow in a subscriber session.
  - Post-Paid at Session Level excluding some flows - Monitoring is done for a subscriber session excluding specific traffic flows.
  - Post-Paid at Flow Level with Multiple flows - Monitoring is done for one or more traffic flows in a subscriber session

  In all Post-Paid scenarios the information on Granted-Service-Unit AVP is not included in Usage-Monitoring-Information AVP. Monitoring and reporting of postpaid session occurs on the following triggers.
  - The subscriber session ends.
  - All the rules associated with the Monitoring-Key charging rule definition are removed.
  - A RAR message is sent to PCRF.
  - Monitoring is disabled by PCRF.

Quota and Threshold

The Granted-Service-Unit AVP contains the following parameters:

- CC-Total-Octets --- Total volume
- CC-Input-Octets --- Uplink volume
- CC-Output-Octets --- Downlink volume
- CC-Input-Octets and CC-Output-Octets --- Uplink and Downlink Volume

Any of the above parameters retrieved from Granted-Service-Unit AVP is termed as Quota.

Levels of Monitoring

Monitoring and reporting of subscriber session usage can be performed at the following levels:

- **Session Level**
  - All traffic flows for a subscriber session
  - All traffic flows for a subscriber session excluding specific traffic flows
- **PCC Rule Level**
  - All traffic flows are monitored for a single PCC Rule
  - All traffic flows are monitored for multiple PCC Rules

Session Level Monitoring or Rule Level Monitoring

Monitoring of a session based on a specific traffic flow can be configured using rules. To enable monitoring of traffic flows using rules, set Usage-Monitoring-Level AVP with RULE_LEVEL (1). You can associate one or more rules with the M onitoring- Key parameter .

To enable session level monitoring, set Usage-Monitoring-Level AVP to value SESSION_LEVEL (0). Monitoring of traffic flows in a session can be activated either when the session loads or when the session is in progress.

Note Monitoring at a RULE level can be enabled only at the time when the rule is installed. It is not possible to enable a rule after the rule installation is done.

Supported AVP for Gx Diameter on ISG

Figure 67: Supported AVP Pair

AVP ID	Name	Type	CCR I	CCR U	CCR T	CCA I	CCA U	CCA T	RAR	RAA
1001	Charging-Rule-Install	Grouped	0	0	0	0-n	0-n	0	0-n	0
2828	-Monitoring-Flags	Unsigned32	0	0	0	0-1	0-1	0	0-1	0
1067	Usage-Monitoring-Information	Grouped	0	0-n	0-n	0-n	0-n	0	0-n	0
1066	• Monitoring-Key	OctetString	-	1	1	1	1	0	1	0
431	• Granted-Service-Unit	Grouped	-	-	-	0-1	0-1	0	0-1	0
421	- CC-Total-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
412	- CC-Input-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
414	- CC-Output-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
446	• Used-Service-Unit	Grouped	0	0-1	0-1	-	-	-	-	0
421	- CC-Total-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
412	- CC-Input-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
414	- CC-Output-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
1068	• Usage-Monitoring-Level	Enumerated	-	-	-	0-1	0-1	0	0-1	0
1069	• Usage-Monitoring-Report	Enumerated	-	-	-	0-1	0-1	0	0-1	0
1070	• Usage-Monitoring-Support	Enumerated	-	-	-	0-1	0-1	0	0-1	0

366725

How to Configure Gx Diameter Monitoring and Reporting

Enable Diameter Configuration

Configure Diameter base configuration with peer details like PCRF IP address and port

To enable diameter configuration:

```
aaa new-model
!
diameter timer watchdog 300
diameter redundancy
diameter origin realm cisco.com
diameter origin host isg-pcef1
diameter source interface GigabitEthernet0/0/0
diameter gx retransmit 3
diameter gx tx-timer 15
!
diameter peer PCRF
 address ipv4 209.165.200.225
 transport tcp port 3868
 source interface GigabitEthernet0/0/0
 timer connection 20
 timer watchdog 100
 timer transaction 20
```

Verifying Diameter Configuration

Use **show diameter peer**command to check for Diameter server connection status. If diameter connection is up and running, the **Peer connection status** field will have value Open. The status Closed indicates that the Diameter server is not functional.

```
Device# show diameter peer PCRF

Peer information for pcrf2
------------------------------
Peer name : PCRF
Peer type : undefined
Peer IP address : 209.165.200.225
Peer transport protocol : TCP
Peer listening port : 3868
Peer security protocol : IPSEC
Peer connection timer value : 10 seconds
Peer watchdog timer value : 300 seconds
Peer transaction timer value : 10 seconds
Peer VRF name :
Peer connected interface : GigabitEthernet0/0/0
Peer destination realm :
Peer destination host name :
Peer connection status : Open


       Peer Statistics
---------------------------------
            IN     /    OUT
---------------------------------
ASR          0             0
ASA          0             0
ACR          0             0
ACA          0             0
CER          0             9
CEA          9             0
DWR          0          5968
DWA       5966             0
DPR          0             2
DPA          2             0
RAR          0             0
RAA          0             0
STR          0             0
STA          0             0

Prot. Errs Sent  :        0     Prot. Errs Rcvd  :           0
Trans. Errs Sent :        0     Trans. Errs Rcvd :           0
Perm. Errs Sent  :        0     Perm. Errs Rcvd  :           0
Conn. Down Errs  :
```

Enable AAA Configuration

Configure AAA authorization method-lists. Authorization method-list is configured with details of the Diameter server

```
aaa new-model
!
aaa authorization policy-if AUTH group SERVER_GROUP1
aaa authorization subscriber-service default local
!
```

```
aaa group server diameter SERVER_GROUP1
    server name PCRF
```

Verifying AAA Configuration

Use show running-config aaa command to display the aaa and diameter configurations.

```
Device##show running-config aaa
aaa authorization subscriber-service default local
aaa authorization policy-if AUTH group SERVER_GROUP1
!
diameter redundancy
diameter origin realm cisco.com
diameter origin host isg-pcef1
diameter source interface GigabitEthernet0/0/0
diameter timer watchdog 300
diameter gx retransmit 3
diameter gx tx-timer 15
!
diameter peer PCRF
 address ipv4 209.165.200.225
 timer connection 20
 timer watchdog 100
 timer transaction 20
 source interface GigabitEthernet0/0/0
!
aaa group server diameter SERVER_GROUP1
server name PCRF

Conn. Down Errs  :
```

Enable ISG Services

Configure the ISG Service with details of network type and initiator

```
ip access-list extended drl_in
 permit ip any any
!
ip access-list extended drl_out
 permit ip any any
!
   class-map type traffic match-any DRL
    match access-group output name drl_out
    match access-group input name drl_in
!
   policy-map type service DRL_TC
    100 class type traffic DRL
    gx-monitoring-key MK1
    police input 20000 50000 70000
    police output 8000 1000 1000
```

Create ISG Control Policy and Associate Policy to Access Interface

Configure the ISG control policy using the following configuration:

```
policy-map type control GX_TEST
 class type control always event session-start
  10 collect identifier source-ip-address
  20 authorize aaa list AUTH identifier <mac-address/source-ip-address/nas-identifier>
```

Associate ISG control policy to access interface

```
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 service-policy type control GX_TEST
 ip subscriber l2-connected
  initiator unclassified mac
  initiator dhcp
```

Configuration Examples on Using Usage-Monitoring-Information AVP

Sample Usage-Monitoring-Information AVP Configuration for Session -Level Traffic Flow

Example: Configuration for Session Level Traffic Flow

```
Usage-Monitoring-Information {
  Monitoring-Key = “Post-Session”
  Usage-Monitoring-Level = “Session-Level”
}
```

Sample Usage-Monitoring-Information AVP Configuration for Monitoring Rule-Level Traffic Flow

Example: Configuration for Monitoring Rule Level Traffic Flow

```
Usage-Monitoring-Information {
  Monitoring-Key = “Post-Rule”
  Usage-Monitoring-Level = “Rule-Level”
}
Charging-Rule-Definition {
  Charging-Rule-Name = “Rule1”
  Monitoring-Key = “Post-Rule”
}
```

Sample Usage-Monitoring-Information AVP Configuration for Monitoring Multiple Traffic Flows

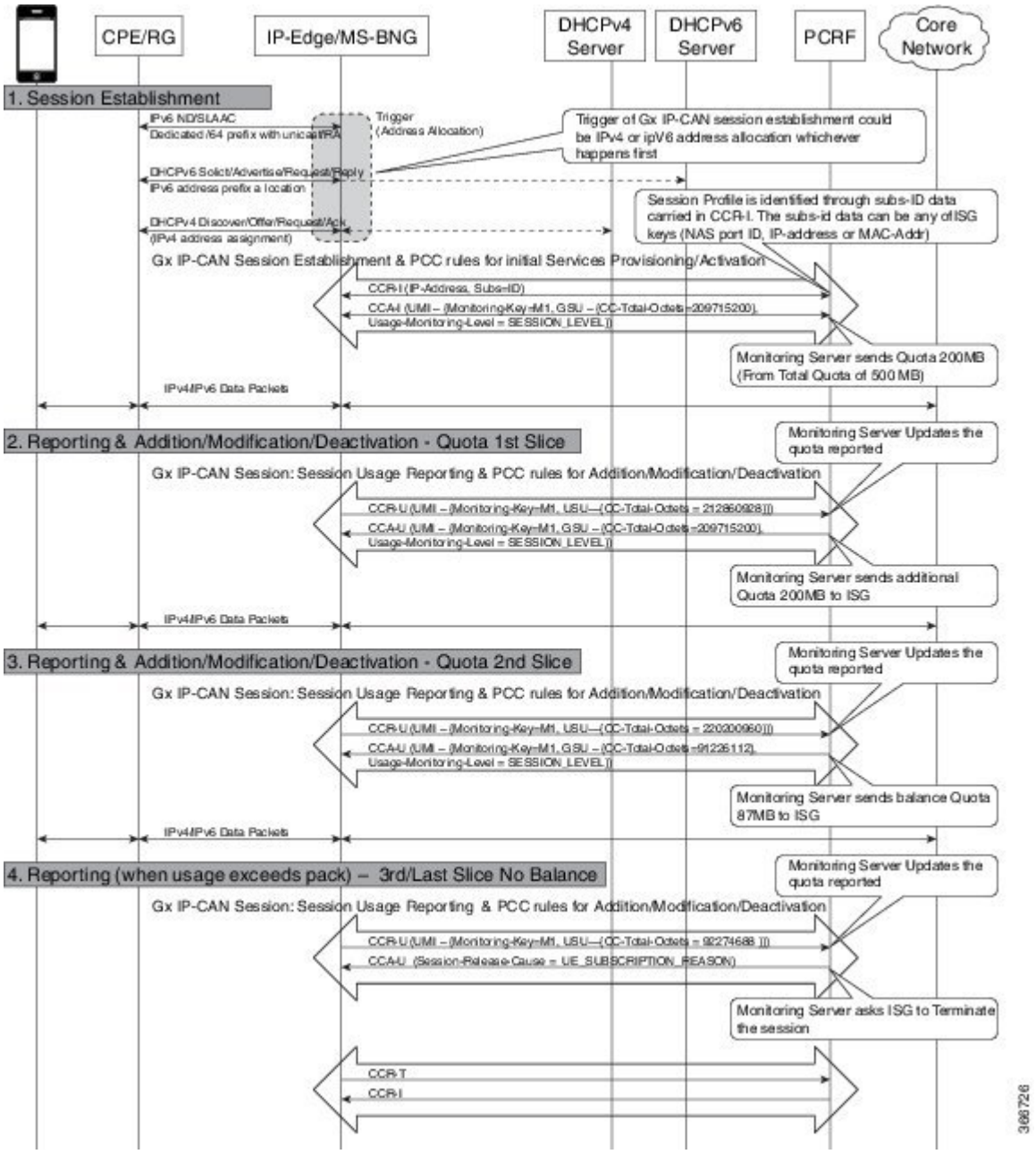
Example: Configuration for Monitoring Multiple Traffic Flows

```
Usage-Monitoring-Information {
```

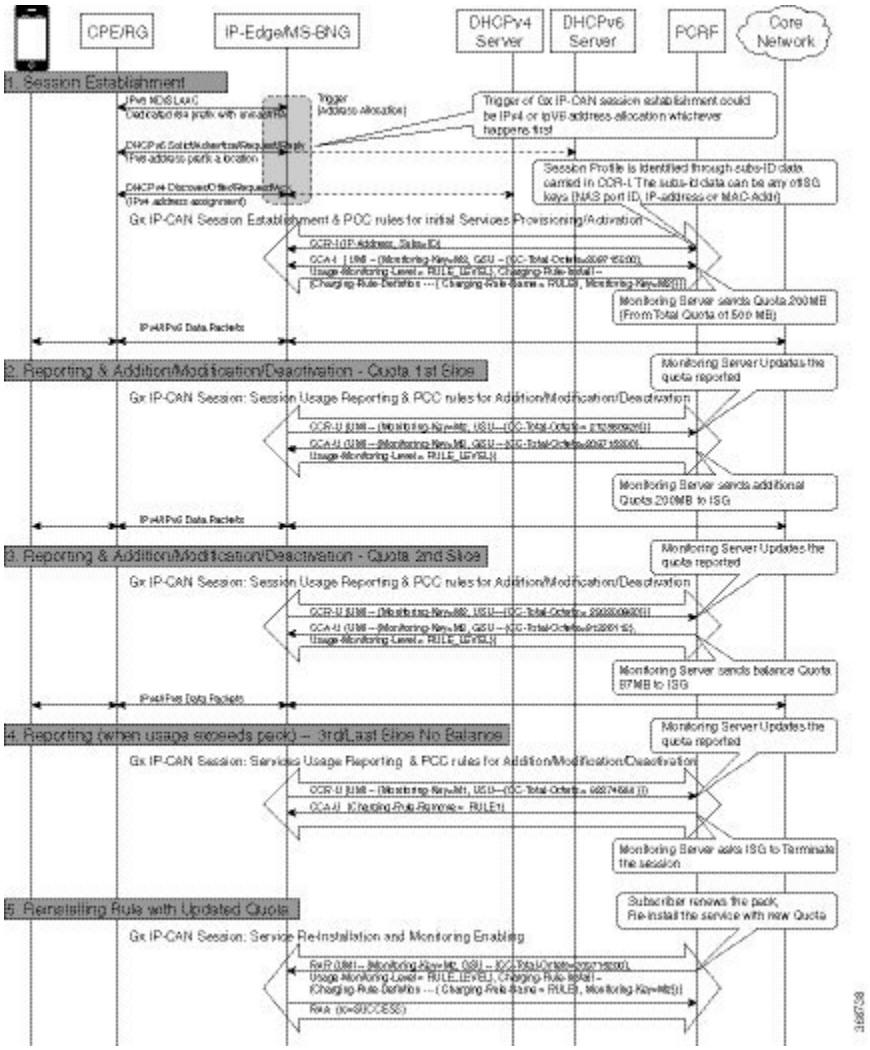
```
  Monitoring-Key = "Post-Session"
  Usage-Monitoring-Level = "Session-Level"
}
Charging-Rule-Install {
  Charging-Rule-Name = "Rule1"
  Charging-Rule-Name = "Rule2"}
```

Monitoring and Reporting Call Flows

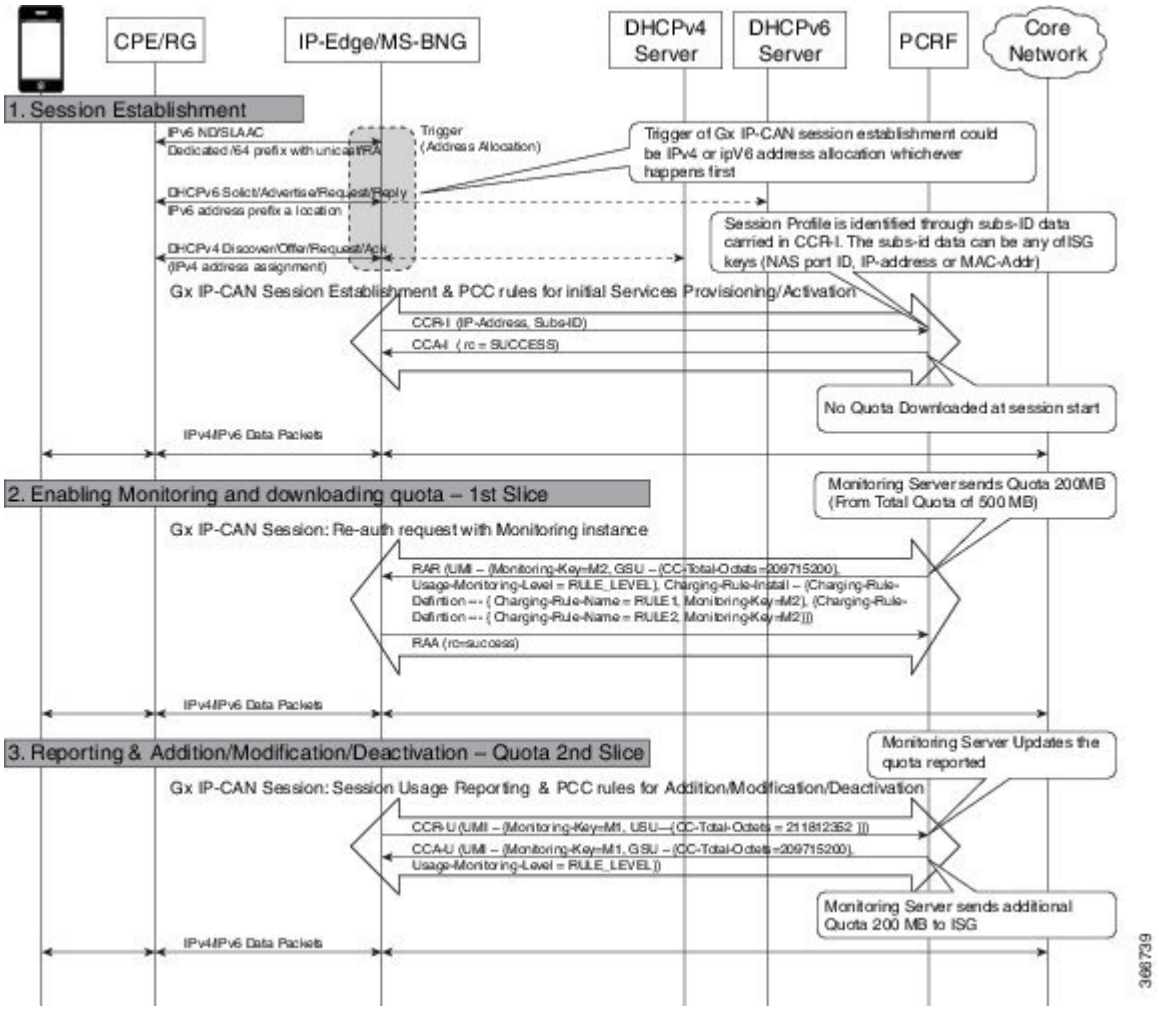
Monitoring Using CCR-When a Session is Loaded



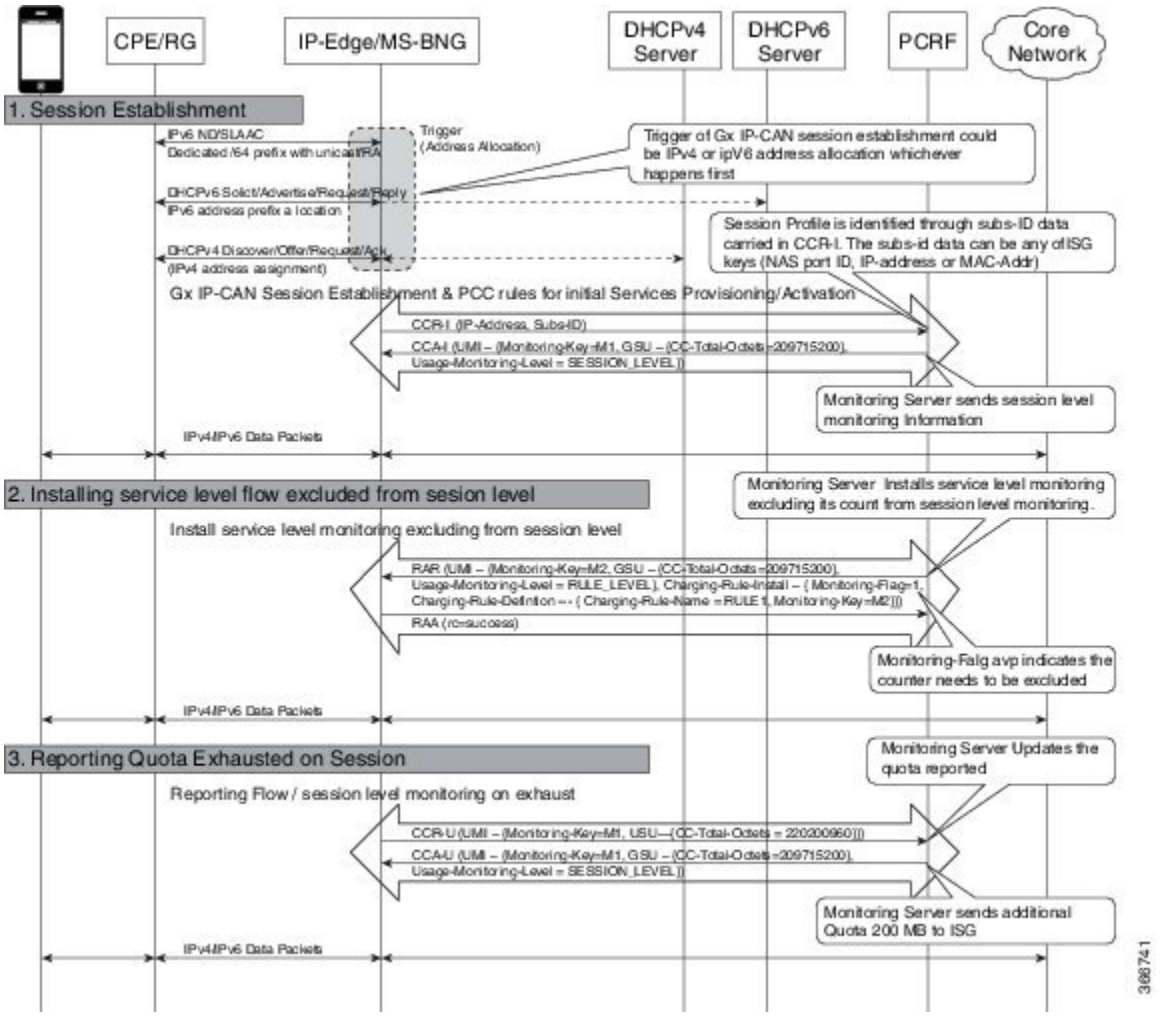
Enabling Service-Level Monitoring and Removing the Rule on Exhaust of Quota



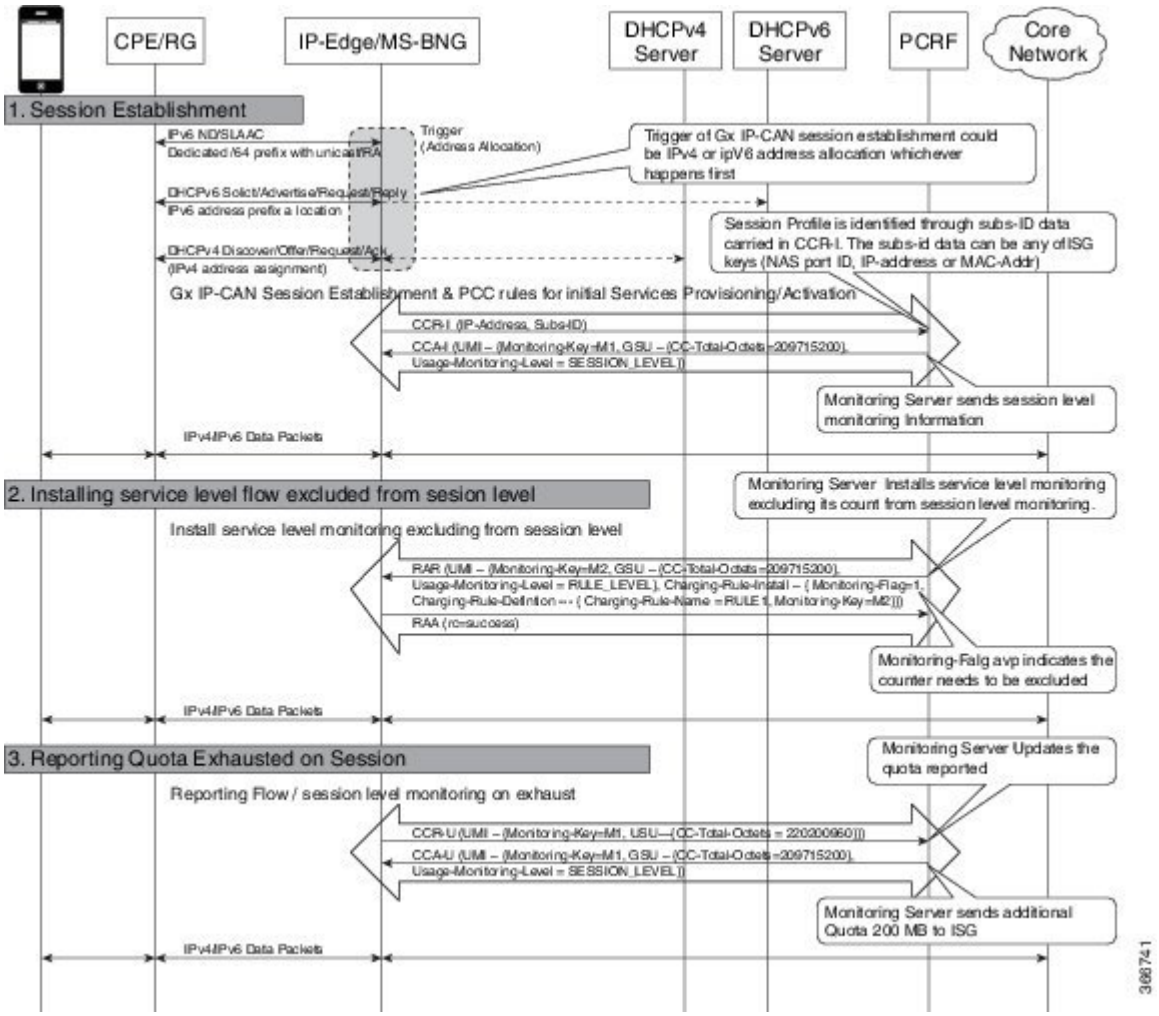
Enabling Monitoring for Multiple Services



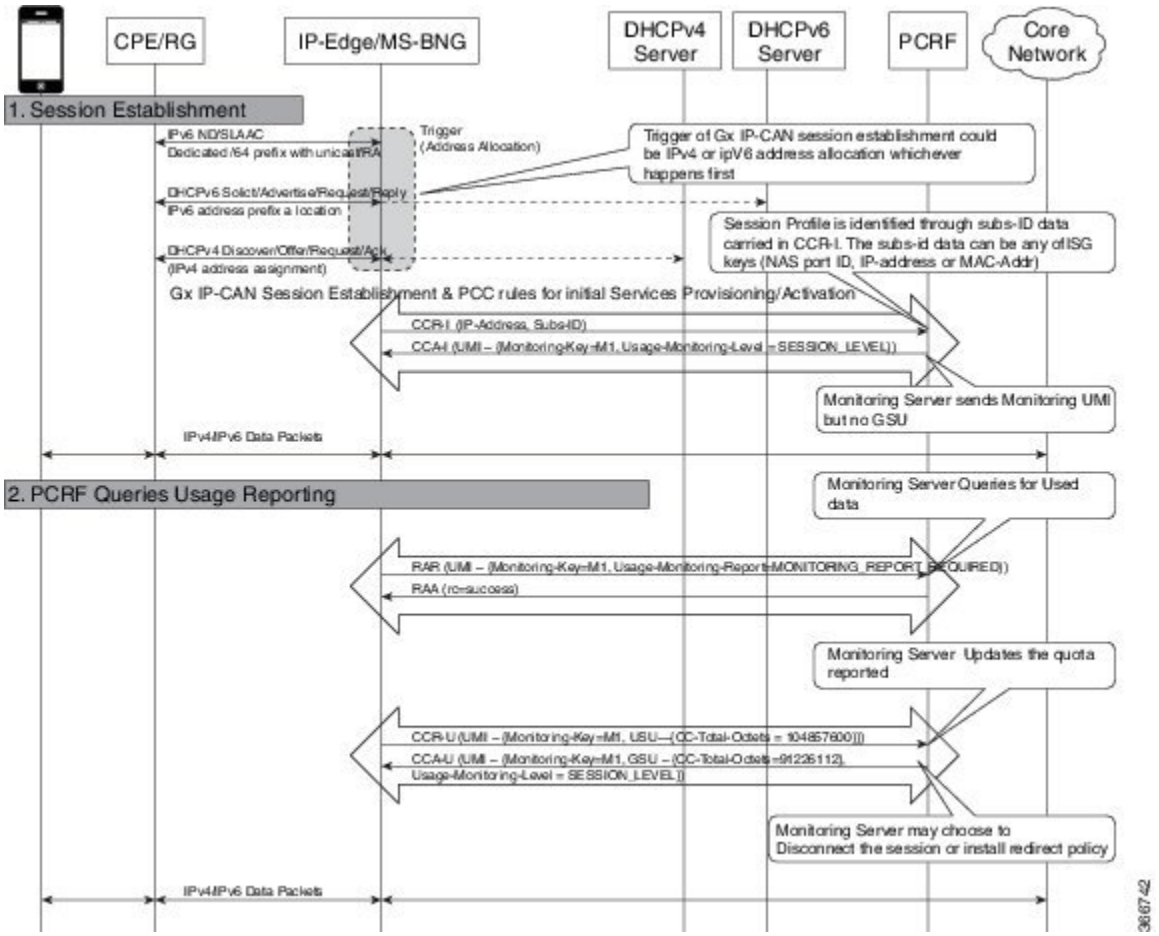
Enabling Session-Level and Service-Level Monitoring



Excluding Session-Level Monitoring from Session Counters



Monitoring Postpaid Services



Additional References for Gx Diameter Monitoring and Reporting

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards and RFCs

Standard/RFC	Title
Standard	*Title*

MIBs

MIB	MIBs Link
• CISCO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Gx Diameter Monitoring and Reporting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 151: Feature Information for Gx Diameter Monitoring and Reporting

Feature Name	Releases	Feature Information
Gx Diameter Monitoring and Reporting	Cisco IOS XE Everest 16.6.1	The Gx Diameter Monitoring and Reporting The following commands were introduced by this feature: **h225**.

CHAPTER 113

DHCPv6 Support for ISG

Dynamic Host Configuration Protocol (DHCP) v6 supports Intelligent Services Gateway (ISG) session as a standalone application for allocating delegated prefixes to Customer Premises Equipment (CPE). The clients behind CPE are allocated addresses from the assigned prefixes.

Restrictions for DHCPv6 Support for ISG

- ISG DHCPv6 IPoE session is initiated only after DHCPv6 transactions and successful IPv6 prefix assignment from DHCPv6 server are complete.
- For DHCPv6, assignment of IANA & IAPD IPv6 prefixes (with any of IPv6 prefix attributes including Delegated-IPv6-Prefix) are not supported through RADIUS.
- ISG IPv6 IPoE sessions are supported with either Stateless Address Auto-Configuration (SLAAC) or DHCPv6 only.
- ISG IPv6 IPoE is not supported for clients connecting through any DHCPv6 Relay Agent as DHCPv6 packets are encapsulated in Relay-Forward or Relay-Reply messages between clients and ISG

Information About DHCPv6 Support for ISG

Interaction with FHS

In the Layer 2 connected subscriber sessions, the first hop security must be enabled This is the main requirement for ISG IPv6 Layer 2 connected subscriber sessions. On configuring control policy on the interface, ISG enables FHS snooping policy.

The First-Hop Security (FHS) intimates ISG about:

- FSoL on binding entry creation in the binding table for messages such as RS, NS, and NA.
- Removal of binding entry from the binding table with disassociation message.
- Data packets which are pushed to RP and not having the binding table entry in FHS.
- Interface change when you move from one interface to another.

ISG does not get information on any other control packets for session initiation.

Existing FHS behavior is modified and programmed to snoop DHCPv6 prefix.

Interaction with IPv6 ND

IPv6 ND sends multicast Router Advertisement (RA) at regular intervals and on receiving Router Solicitation (RS) from the host on bootup with all IPv6 prefixes. The interaction between the IPv6 ND and ISG happens with ISG integration. IPv6 ND sends unicast RA, instead of multicast RA, with prefixes assigned to the subscriber.

In case of DHCPv6, unicast RA is not advertised to client containing the prefix, to support this feature. Based on the type of the session (SLAAC or DHCPv6) ISG enables or disables RA session respectively.

Support for DHCPv6 Single or Dual Stack Session Bringup

To support ISG dual stack sessions with DHCPv6, an interface is configured with ISG and FHS is programmed for prefix-glean snooping policy. After the DHCPv6 handshake, a prefix is allocated to the CPE. Binding for the assigned prefix is created in FHS and a notification is sent to the IPSUB along with the prefix.

ISG session initiator unclassified-mac is used to support DHCPv6. After the DHCPv6 handshake is complete, a binding is created in FHS and a notification is sent to trigger an IPSUP session.

Based on the configuration on the interface, ISG configuration handler will program FHS for SLAAC or DHCPv6 based sessions.

For DHCPv6, ISG session is provisioned for MAC-address of the CPE and the prefix is allocated through DHCPv6. So the DHCP session is provisioned for the CPE MAC and DHCPv6. Packets flowing from the clients allocated IP address through this delegated prefix is accounted for this session.

How to Configure DHCPv6 Support for ISG

Configuration for DHCPv6 Support for ISG

Perform the following task to configure DHCPv6 support for ISG.

```
interface Port-channel8.10
    encapsulation dot1Q 10 primary GigabitEthernet1/1/0
    ip address 192.168.11.1 255.255.255.0
    ipv6 address 3002::1/64
    ipv6 enable
    ipv6 nd managed-config-flag
    ipv6 nd other-config-flag
    ipv6 dhcp relay destination 201:201:201:201::2
    service-policy type control GX_TEST
    ip subscriber l2-connected
```

```
initiator unclassified mac-address
initiator dhcp
```

Configuration Examples for DHCPv6 Support for ISG

Example: DHCPv6 Support for ISG

Example: DHCPv6 Support for ISG

```
Device# show ipv6 neighbors binding
Binding Table has 3 entries, 1 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API
- API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


        IPv6 address                                            Link-Layer addr
Interface        vlan prlvl  age   state    Time left
L      FE80::A8BB:CCFF:FE02:F800                AABB.CC02.F800       Et0/0             0
0100   24mn REACHABLE
L      ABCD::1                                                  AABB.CC02.F800
Et0/0             0  0100   24mn REACHABLE
DH  2010::/64                                                AABB.CC02.9401        Et0/0
             0  0024   24mn REACHABLE
```

Additional References for DHCPv6 Support for ISG

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
• CISCO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCPv6 Support for ISG

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 152: Feature Information for DHCPv6 Support for ISG

Feature Name	Releases	Feature Information
DHCPv6 Support for ISG	Cisco IOS XE Everest 16.5.1b	This feature is about DHCPv6 Support for ISG. There were no commands introduced or modified in this feature.
Unclassified MAC Initiator with IANA	Cisco IOS XE Gibraltar 16.12.1	ISG IPv6 sessions are based on the unclassified mac address of the subscriber. If you use DHCPv6 for IPv6 addresses, ISG creates subscriber sessions based on DHCPv6 packets with the IANA option.

CHAPTER 114

DHCP RADIUS Proxy for ISG

The DHCP RADIUS Proxy for ISG feature enables the support for downloading DHCP parameters from RADIUS and use these parameters to configure the DHCP client.

Information About DHCP RADIUS Proxy for ISG

DHCP RADIUS Proxy for ISG

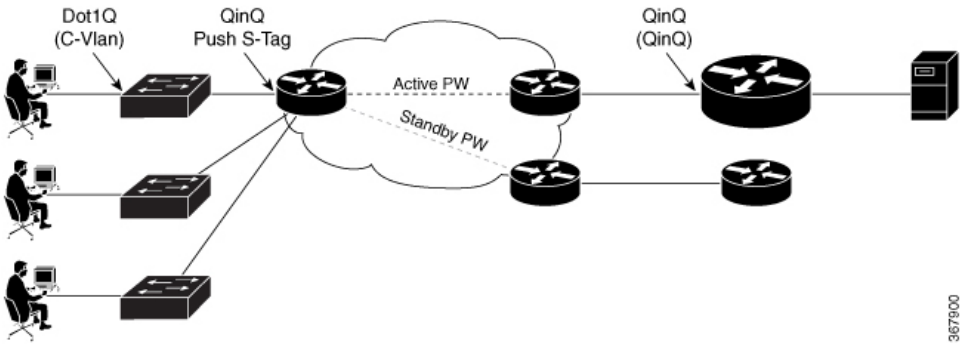
When ISG is in the path of DHCP requests, ISG can influence the IP address pool and DHCP servers that are used to assign subscriber IP addresses. This is achieved by configuring a DHCP address pool. As a result on a per-request basis, an IP address is either provided by local DHCP server or relayed to a remote DHCP server that is defined in selected pool.

The DHCP RADIUS Proxy with ISG feature enables downloading of the DHCP parameters like IPv4 address, mask, lease time, and so on from RADIUS as part of the Access-Accept message. DHCP RADIUS Proxy with ISG feature supports allocation of client IP addresses using parameters that are downloaded using RADIUS or using locally configured pool.

Note If static IP is provided by RADIUS, then it must be used to configure the client. If Static IP is not provided, IP is allocated dynamically using the locally configured pool or using Relay.

DHCP RADIUS Proxy for ISG Topology

Figure 68: DHCP RADIUS Proxy for ISG Topology



In the above figure:

- End user sends DHCP-Discover message to ISG.
- To initiate session based on DHCP, ISG asks RADIUS with Access-Request
- RADIUS answers with Access-Accept and sends static IP address (RADIUS Attribute 8 Framed-IP-Address) and other parameters like lease time, gateway, and so on.
- ISG receives this Accept message, parses the address, adds DHCP binding for this subscriber, and sends DHCP Offer with proposed IP address and other DHCP parameters (Lease Time and Gateway).
- ISG starts the new subscriber session.

Prerequisites for DHCP RADIUS Proxy for ISG

- The downloaded IP must confine to the following:
  - The downloaded IP address subnet mask must be part of an address-pool.
  - The client interface must be on the same subnet as that of the downloaded IP for non-VRF case.
- The IP addresses that are provided by RADIUS must be part of the configured range of excluded address, so as to to prevent dynamic DHCP from allocating the same IP address vice-versa.
- All parameters provided by RADIUS must override the same options present in the locally configured pool on the interface.

Restrictions for DHCP RADIUS Proxy for ISG

- VRF transfer with DHCP Radius Proxy is not supported. VRF transfer in ISG is achieved using ISG service login. Per-user DHCP data like IP Address, Subnet Mask, Lease-time, Gateway, and so on cannot be defined or passed using service definition.
- Service is global and can be applied to multiple customers.
- Only Layer 2-connected DHCP sessions are supported.

- Dual stack sessions are not supported.

How to Configure DHCP RADIUS Proxy for ISG

Configuring DHCP RADIUS Proxy

The following RADIUS parameters can be downloaded to trigger DHCP Radius Proxy feature:

```
Cleartext-Password := "cisco"
               Service-Type = Framed-User,
               Framed-IP-Address = 10.0.0.3,
               Framed-IP-Netmask = 255.255.0.0,
               Framed-Route += "192.0.2.1 255.255.255.0 203.0.113.1",
               Cisco-AVPair += "ip:lease-duration=600",
               Cisco-AVPair += "ip:default-ipv4-gateway=10.0.0.1",
               Cisco-AVPair += "ip:primary-dns=10.40.0.1",
               Cisco-AVPair += "ip:secondary-dns=10.0.0.2",
               Cisco-AVPair += "ip:vrf-id=RED",
               Cisco-AVPair += "subscriber:classname=dhcp-red-class",
```

Verifying RADIUS-Based Policing

Use the following command to find if the DHCP IP Address is assigned dynamically or through RADIUS Proxy.

Note The Type field for RADIUS Proxy is ISG if IP address is obtained from RADIUS. If IP address is assigned from local pool, the Type field is Automatic.

```
Device# show ip dhcp binding
Bindings from VRF pool RED:
IP address      Client-ID/                    Lease expiration            Type       State
      Interface Hardware address/ User name

10.0.0.3        0100.0000.0000.03        May 21 2017 02:56 AM         ISG        Active
  multiservice0
```

Additional References for DHCP RADIUS Proxy for ISG

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
• CISCO-AAA-SERVER-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCP RADIUS Proxy for ISG

Table 153: Feature Information for DHCP RADIUS Proxy for ISG

Feature Name	Releases	Feature Information
DHCP RADIUS Proxy for ISG	Cisco IOS XE Gibraltar 16.10.1	The DHCP RADIUS Proxy for ISG feature enables the support for downloading DHCP parameters from RADIUS and use these parameters to configure the DHCP client.