



Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide

Cisco IOS XE Release 3S

Americas Headquarters

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2009-2011 Cisco Systems, Inc. All rights reserved.



Broadband Access Aggregation Overview



Preparing for Broadband Access Aggregation

First Published: May 2, 2005
Last Updated: August 11, 2009

Before you begin to perform the tasks required to accomplish broadband access aggregation, there are some preparatory tasks that you can perform at your option to enable you to complete the aggregation task with more efficiency.

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.

Finding Feature Information

For the latest feature information and caveats, see 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 for Preparing for Broadband Access Aggregation” section on page 11](#).

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



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

- [Restrictions for Preparing for Broadband Access Aggregation, page 2](#)
- [Information About Preparing for Broadband Access Aggregation, page 2](#)
- [How to Prepare for Broadband Access Aggregation, page 4](#)
- [Configuration Examples for Preparing for Broadband Access Aggregation, page 6](#)
- [Additional References, page 9](#)
- [Feature Information for Preparing for Broadband Access Aggregation, page 11](#)

Restrictions for Preparing for Broadband Access Aggregation

The following restriction apply:

- 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.

Information About Preparing for Broadband Access Aggregation

To prepare for broadband access aggregation, you should understand the following concepts:

- [Virtual Access Interfaces, page 2](#)
- [Configuration Enhancements for Broadband Scalability, page 3](#)

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

This section contains the following procedures:

- [Configuring a Virtual Template Interface, page 4](#)
- [Configuring Enhancements for Broadband Scalability, page 5](#)

Configuring a Virtual Template Interface

Configure a virtual template before you configure PPPoE on a Gigabit Ethernet interface. The virtual template interface is a logical entity that is applied dynamically as needed to an incoming PPP session request. To create and configure a virtual template interface, enter the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ip unnumbered loopback** *number*
5. **mtu** *bytes*
6. **ppp authentication chap**
7. **ppp ipcp ip address required**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface virtual-template <i>number</i> Example: Router(config)# interface virtual-template 1	Creates a virtual template interface and enters interface configuration mode.
Step 4	ip unnumbered loopback <i>number</i> Example: Router(config-if)# ip unnumbered loopback 0	Enables IP without assigning a specific IP address on the LAN.

	Command or Action	Purpose
Step 5	<p><code>mtu bytes</code></p> <p>Example: Router(config-if)# mtu 1492</p>	<p>(Optional) Sets the maximum MTU size for the interface.</p> <p>Note MTU size can be set only to 1492 or 1500. To set MTU size greater than 1492, you must use the tag ppp-max-payload command.</p>
Step 6	<p><code>ppp authentication chap</code></p> <p>Example: Router(config-if)# ppp authentication chap</p>	<p>Enables PPP authentication on the virtual template interface.</p>
Step 7	<p><code>ppp ipcp ip address required</code></p> <p>Example: Router(config-if)# ppp ipcp ip address required</p>	<p>Prevents a PPP session from being set up without a valid address being negotiated.</p> <p>This command is required for legacy dialup and DSL networks.</p>

Examples

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

```
interface virtual-template 1
 ip unnumbered Loopback 0
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
```

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, page 5](#)

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	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>test virtual-template template subinterface</code> 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

This section provides the following configuration examples:

- [Virtual Access Subinterfaces Configuration: Examples, page 6](#)

Virtual Access Subinterfaces Configuration: Examples

This section provides the following configuration examples:

- [Virtual Access Subinterface Configuration: Example, page 7](#)
- [Testing a Virtual Template for Compatibility with Subinterfaces: Example, page 8](#)

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 tunnell
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	<i>Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions</i>
Specifying a range for the ppp-max payload tag value	<i>PPP-Max-Payload and IWF PPPoE Tag Support</i>
Additional information about commands used in this document	<ul style="list-style-type: none"> • <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i> • <i>Cisco IOS Master Command List, All Releases</i>

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Preparing for Broadband Access Aggregation

Table 4 lists the features in this module and provides links to specific configuration information

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 4 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 4 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	<p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring Enhancements for Broadband Scalability, page 5 • Virtual Access Subinterfaces Configuration: Examples, page 6

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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.

© 2005–2009 Cisco Systems, Inc. All rights reserved.



PPPoE



PPPoE Circuit-Id Tag Processing

First Published: February 14, 2006
Last Updated: May 4, 2009

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.

Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE Circuit-Id Tag Processing” section on page 10](#).

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

Contents

- [Prerequisites for the PPPoE Circuit-Id Tag Processing Feature, page 2](#)
- [Information About the PPPoE Circuit-Id Tag Processing Feature, page 2](#)
- [How to Configure the PPPoE Circuit-Id Tag Processing Feature, page 4](#)
- [Configuration Examples for the PPPoE Circuit-Id Tag Processing Feature, page 8](#)
- [Additional References, page 9](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for the PPPoE Circuit-Id Tag Processing Feature

It is recommended that you be familiar with RFC 2516 before configuring this feature. See the [“RFCs” section on page 9](#) for a pointer to this standard.

Information About the PPPoE Circuit-Id Tag Processing Feature

To configure the PPPoE Circuit-Id Tag Processing feature, you should understand the following concepts:

- [Differences Between ATM- and Fast or Gigabit Ethernet-Based Broadband Access Networks, page 2](#)
- [DSL Forum 2004-71 Solution, page 2](#)
- [Approach for a Circuit-Id Tag in Ethernet-Based Broadband Access Networks, page 3](#)
- [Benefits of the PPPoE Circuit-Id Tag Processing Feature, page 4](#)

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” section on page 8](#) for an example.

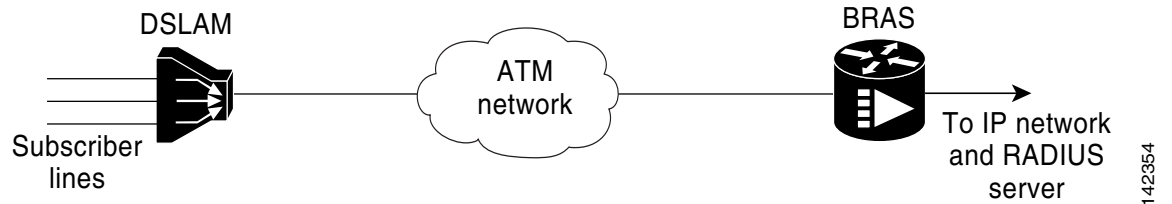
DSL Forum 2004-71 Solution

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 [Figure 1](#).

Figure 1 ATM-Based DSL Broadband Access Network

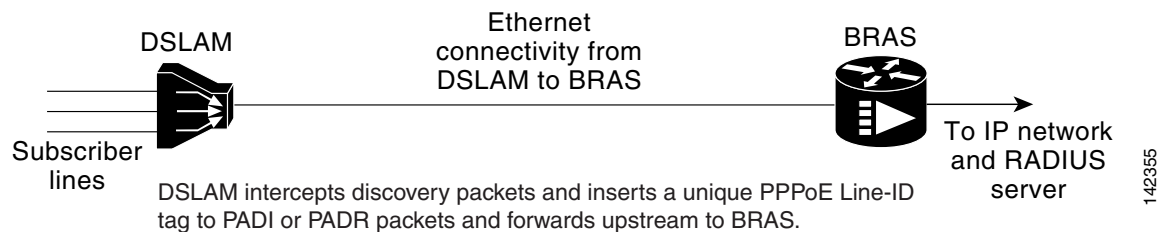


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM VC used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-Id for use in RADIUS packets.

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 [Figure 2](#). 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 2 PPPoE Circuit-Id Tag Processing Solution



DSLAM intercepts discovery packets and inserts a unique PPPoE Line-ID tag to PADI or PADR packets and forwards upstream to BRAS.

BRAS processes the tag and extracts the Remote-ID, which is stored on the session.

The Remote-ID is sent as a NAS-Port-ID attribute in AAA accounting and PPP authentication requests.

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

This section contains the following procedures:

- [Configuring the PPPoE Circuit-Id Tag Processing Feature, page 4](#) (Required)
- [Removing the PPPoE Circuit-Id Tag, page 5](#) (Required)
- [Displaying the Session Activity Log, page 6](#) (Optional)

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” section on page 2](#)) 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. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	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. <ul style="list-style-type: none"> 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” and “Configuring PPPoE Circuit-Id Tag Processing: Example” 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: Router(config-bba-group)# vendor-tag circuit-id service	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.

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

- enable**
- configure terminal**
- bba-group pppoe group-name**
- vendor-tag strip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>bba-group pppoe group-name</code> Example: Router(config)# bba-group pppoe pppoe-group	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	<code>vendor-tag strip</code> 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”](#) section on page 8 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 Access
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 = 0/0/200
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 "0/0/200_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

```

SUMMARY STEPS

1. enable
2. debug radius

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>debug radius</code> Example: Router# debug radius	Displays a report of session activity.

Configuration Examples for the PPPoE Circuit-Id Tag Processing Feature

This section contains the following examples:

- [Configuring PPPoE Circuit-Id Tag Processing: Example, page 8](#)
- [Configuring BRAS to Include a NAS-Port-Id Attribute: Example, page 8](#)
- [Removing the PPPoE Circuit-Id Tag: Example, page 9](#)

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for PPPoE Circuit-Id Tag Processing

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for PPPoE Circuit-Id Tag Processing

Feature Name	Releases	Feature Information
PPPoE Circuit-Id Tag Processing	Cisco IOS XE Release 2.1.	<p>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.</p> <p>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>This feature was integrated into Cisco IOS XE Release 2.3.1.</p> <p>The following commands were introduced or modified: vendor-tag circuit-id service, vendor-tag strip.</p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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.

© 2006–2009 Cisco Systems, Inc. All rights reserved.



Configuring PPP over Ethernet Session Limit Support

First Published: May 4, 2005

Last Updated: November 17, 2010

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Configuring PPP over Ethernet Session Limit Support”](#) section on page 10.

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

Contents

- [Information About Configuring PPP over Ethernet Session Limit Support, page 2](#)
- [How to Configure PPP over Ethernet Session Limit Support, page 2](#)
- [Configuration Examples for PPP over Ethernet Session Limit Support, page 7](#)
- [Additional References, page 8](#)
- [Feature Information for Configuring PPP over Ethernet Session Limit Support, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Configuring PPP over Ethernet Session Limit Support

- [Benefits of Configuring PPP over Ethernet Session Limit Support, page 2](#)
- [Trap Generation, page 2](#)

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, page 2](#) (optional)
- [Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface, page 4](#) (optional)
- [Configuring System-Wide Threshold Parameters, page 5](#) (required)

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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	bba-group pppoe { <i>name</i> global }	Configures a broadband aggregation (BBA) group to be used to establish PPPoE sessions and enters BBA group configuration mode. <ul style="list-style-type: none"> • <i>name</i>—Name of the BBA group. You can have multiple BBA groups. • 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 <i>template-number</i> 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 <i>per-mac-limit</i> 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.

	Command or Action	Purpose
Step 6	<p>sessions per-vlan limit <i>per-vlan-limit</i> [inner <i>vlan-id</i>]</p> <p>Example: Router(config-bba-group)# session per-vlan limit 4000 inner 3500</p>	<p>(Optional) Sets the session limit for the inner VLAN on QinQ subinterface. The default session limit is 100.</p> <p>Note The per-VLAN limit is only applicable to Gigabit Ethernet subinterfaces (802.1q VLANs).</p>
Step 7	<p>sessions per-vc limit <i>per-vc-limit</i> [threshold <i>threshold-value</i>]</p> <p>Example: Router(config-bba-group)# sessions per-vc limit 2000</p>	<p>(Optional) Sets the maximum number of PPPoE sessions allowed per VC session limit in a PPPoE profile. The default session limit is 100.</p> <p>Note The per-VC limit is applicable only to ATM interfaces and subinterfaces.</p>
Step 8	<p>sessions max limit <i>number-of-sessions</i> [threshold <i>threshold-value</i>]</p> <p>Example: Router(config-bba-group)# sessions max limit 32000</p>	<p>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.</p> <p>Note This command applies only to the global profile.</p>
Step 9	<p>exit</p> <p>Example: Router(config-bba-group)# exit</p>	<p>Returns to global configuration mode.</p>

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} <i>slot/subslot/port[.subinterface]</i> 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

Perform this task to configure the system-wide threshold parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe global**
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 pppoe global 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: Router(config-if)# pppoe-sessions threshold 1000	Configures per-session threshold value.
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

This section provides the following configuration examples:

- [Example: Specifying the Maximum Number of PPPoE Sessions on a Router, page 7](#)
- [Example: Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface, page 7](#)
- [Example: Configuring the System-wide Threshold Parameters, page 7](#)

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	<i>Cisco IOS Master Commands List, All Releases</i>
Broadband and DSL commands	<i>Cisco IOS Broadband and DSL Command Reference</i>
Broadband access aggregation of PPPoE sessions	<i>Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions</i>

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
<p>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.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Configuring PPP over Ethernet Session Limit Support

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 1 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.

Table 1 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	<p>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>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.</p> <p>This feature was integrated into Cisco IOS XE Release 2.4.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Configuring PPP over Ethernet Session Limit Support, page 2 • How to Configure PPP over Ethernet Session Limit Support, page 2
SNMP Enhancements for ASR 1000	Cisco IOS XE Release 3.2S	<p>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.</p> <p>This feature was introduced in Cisco IOS XE 3.2S.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About Configuring PPP over Ethernet Session Limit Support, page 2 • How to Configure PPP over Ethernet Session Limit Support, page 2 <p>The following commands were introduced or modified: pppoe-sessions threshold, sessions threshold.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2005–2010 Cisco Systems, Inc. All rights reserved.



PPPoE Session Limit Local Override

First Published: June 28, 2007

Last Updated: March 2, 2009

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.

Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE Session Limit Local Override” section on page 6](#).

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

Contents

- [Information About PPPoE Session Limit Local Override, page 2](#)
- [How to Configure PPPoE Session Limit Local Override, page 3](#)
- [Configuration Examples for PPPoE Session Limit Local Override, page 4](#)
- [Additional References, page 4](#)
- [Feature Information for PPPoE Session Limit Local Override, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About PPPoE Session Limit Local Override

To configure the PPPoE Session Limit Local Override feature, you should understand the following concept:

- [How PPPoE Session Limit Local Override Works](#)

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

This section contains the following procedures:

- [Enabling PPPoE Session Limit Local Override, page 3](#)

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.

Restrictions

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. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	bba-group pppoe { <i>group-name</i> global } Example: Router(config)# bba-group pppoe test	Creates a PPPoE profile and enters BBA group configuration mode. <ul style="list-style-type: none">• <i>group-name</i>—Name of the PPPoE profile.
Step 4	sessions per-vlan limit <i>per-vlan-limit</i> Example: Router(config-bba-group)# sessions per-vlan limit 3	Limits the number of PPPoE sessions per VLAN in a PPPoE profile. <ul style="list-style-type: none">• <i>per-vlan-limit</i>—Maximum number of PPPoE sessions that can be established over an Ethernet VLAN. The default is 100.

	Command or Action	Purpose
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

This section contains the following examples:

- [Enabling PPPoE Session Limit Local Override: Example](#)

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	<ul style="list-style-type: none"> • Cisco IOS Broadband Access Aggregation and DSL Command Reference • Cisco IOS Master Command List, All Releases

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for PPPoE Session Limit Local Override

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for PPPoE Session Limit Local Override

Feature Name	Releases	Feature Information
PPPoE—Session Limit Local Override	Cisco IOS XE Release 2.1	<p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>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.</p> <p>The following commands were introduced or modified: sessions pre-auth limit ignore.</p>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

First Published: May 2, 2005
Last Updated: March 25, 2011

PPP over Ethernet (PPPoE) profiles contain configuration information for a group of 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 PVCs that are used in supporting broadband access aggregation of PPPoE sessions.



Note

This module describes the method for configuring PPPoE sessions using profiles.

Finding Feature Information

For the latest feature information and caveats, see 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 for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions”](#) section on page 23.

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

Contents

- [Prerequisites for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions, page 2](#)
- [Restrictions for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions, page 2](#)
- [Information About Providing Protocol Support for Broadband Access Aggregation for PPPoE Sessions, page 3](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [How to Provide Protocol Support for Broadband Access Aggregation of PPPoE Sessions](#), page 4
- [Configuration Examples for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions](#), page 16
- [Where to Go Next](#), page 20
- [Additional References](#), page 21
- [Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions](#), page 23

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 [Table 1](#):

Table 1 *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 http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp1045661
Per Subscriber Firewall on PTA	Not supported
Per Subscriber NAT	Not supported
Per Subscriber PBR	Supports up to 1000 sessions from Cisco IOS XE Release 3.1S
Per Subscriber NBAR	Not supported
Per Subscriber Multicast	Supports upto 3,000 sessions from Cisco IOS XE Release RLS 2.2.1 http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp1105824
Per Subscriber Netflow	Not supported
MLPPP on LNS	Not supported
MLPoE on PTA	Not supported

Feature Name	Support Release
MLPoE LAC Switching	Not supported
VLAN range	Not supported

Information About Providing Protocol Support for Broadband Access Aggregation for PPPoE Sessions

To provide protocol support for broadband access aggregation for PPPoE sessions, you should understand the following concepts:

- [PPPoE Specification Definition, page 3](#)
- [PPPoE Connection Throttling, page 3](#)
- [Autosense for ATM PVCs, page 3](#)

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.

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.

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. The profile definition is required as described in the [“Defining a PPPoE Profile” section on page 4](#), and an additional task makes an assignment of the profile to a protocol type.

- [Defining a PPPoE Profile, page 4](#) (required)
- [Enabling PPPoE on an Interface, page 6](#) (required)
- [Assigning a PPPoE Profile to an ATM PVC, page 7](#) (optional)
- [Assigning a PPPoE Profile to an ATM PVC Range and PVC Within a Range, page 8](#) (optional)
- [Assigning a PPPoE Profile to an ATM VC Class, page 10](#) (optional)
- [Configuring Different MAC Addresses on PPPoE, page 11](#) (optional)

When configuring PPPoE session recovery after a system reload, perform the following task:

- [Configuring Different MAC Addresses on PPPoE, page 11](#) (optional)

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}* **throttle** *session-request 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 <i>{group-name global}</i> 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 <i>template-number</i> 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 <i>number-of-sessions</i> [threshold <i>threshold-value</i>] 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 <i>per-mac-limit</i> Example: Router(config-bba-group)# sessions per-mac limit 2	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.
Step 7	sessions per-vlan limit <i>per-vlan-limit inner per-inner-vlan-limit</i> 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 <i>per-vc-limit</i> [threshold <i>threshold-value</i>] 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.

	Command or Action	Purpose
Step 9	sessions { <i>per-mac</i> <i>per-vc</i> } throttle <i>session-requests session-request-period</i> <i>blocking-period</i> 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 VC or a MAC address within a specified period of time.
Step 10	ac name <i>name</i> 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

Perform this task to enable PPPoE on a Gigabit Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *number*
4. **pppoe enable** [*group group-name*]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	<p>pppoe enable [group <i>group-name</i>]</p> <p>Example: Router(config-subif)# pppoe enable group one</p>	<p>Enables PPPoE sessions on an Gigabit Ethernet interface or subinterface.</p> <p>Note If a PPPoE profile is not assigned to the interface by using the group <i>group-name</i> option, the interface will use the global PPPoE profile.</p>
Step 5	<p>end</p> <p>Example: Router(config-subif)# end</p>	<p>(Optional) Exits subinterface configuration mode and returns to privileged EXEC mode.</p>

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. **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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface 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 vpi/vci Example: Router(config-if)# pvc 2/101	Creates an ATM PVC and enters ATM virtual circuit configuration mode.
Step 5	protocol pppoe [group group-name] or encapsulation aal5autopp virtual-template number [group group-name] Example: Router(config-if-atm-vc)# protocol pppoe group one or Router(config-if-atm-vc)# encapsulation aal5autopp 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: Router(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-vpilstart-vci end-vpilend-vci**

5. **protocol pppoe** [**group** *group-name*]
or
encapsulation aal5autopp **virtual-template** *number* [**group** *group-name*]
6. **pvc-in-range** [*pvc-name*] [[*vpi*]/*vci*]
7. **protocol pppoe** [**group** *group-name*]
or
encapsulation aal5autopp **virtual-template** *number* [**group** *group-name*]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface atm <i>number</i> [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 [<i>range-name</i>] pvc <i>start-vpi/start-vci</i> <i>end-vpi/end-vci</i> Example: Router(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 <i>group-name</i>] or encapsulation aal5autopp virtual-template <i>number</i> [group <i>group-name</i>] Example: Router(config-if-atm-range)# protocol pppoe group one or Router(config-if-atm-range)# encapsulation aal5autopp virtual-template 1 group one	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 <i>group-name</i> option, the PVCs in the range will use the global PPPoE profile.

	Command or Action	Purpose
Step 6	<p>pvc-in-range [<i>pvc-name</i>] [[<i>vpi</i>/<i>vci</i>]</p> <p>Example: Router(config-if-atm-range)# pvc-in-range pvc1 3/104</p>	Defines an individual PVC within a PVC range and enables ATM PVC-in-range configuration mode.
Step 7	<p>protocol pppoe [group <i>group-name</i>]</p> <p>or</p> <p>encapsulation aal5autopp virtual-template <i>number</i> [group <i>group-name</i>]</p> <p>Example: Router(config-if-atm-range-pvc)# protocol pppoe group two</p> <p>or</p> <p>Router(config-if-atm-range-pvc)# encapsulation aal5autopp virtual-template 1 group two</p>	<p>Enables PPPoE sessions to be established on a PVC within a range.</p> <p>or</p> <p>Configures PPPoE autosense.</p> <p>Note If a PPPoE profile is not assigned to the PVC by using the group <i>group-name</i> option, the PVC will use the global PPPoE profile.</p>
Step 8	<p>end</p> <p>Example: Router(cfg-if-atm-range-pvc)# end</p>	(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. **protocol pppoe** [**group** *group-name*]
or
encapsulation aal5autopp virtual-template *number* [**group** *group-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vc-class atm <i>vc-class-name</i> Example: Router(config)# vc-class atm class1	Creates an ATM VC class and enters ATM VC class configuration mode. <ul style="list-style-type: none"> A VC class can be applied to an ATM interface, subinterface, or VC.
Step 4	protocol pppoe [group <i>group-name</i>] or encapsulation aal5autopp virtual-template <i>number</i> [group <i>group-name</i>] Example: Router(config-vc-class)# protocol pppoe group two or Router(config-vc-class)# encapsulation aal5autopp 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 <i>group-name</i> option, the PPPoE sessions will be established with the global PPPoE profile.
Step 5	end Example: Router(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 router to bridge packets from Gigabit Ethernet to the appropriate PVC.

Prerequisites for Configurable MAC Address for PPPoE

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 router to bridge packets from Gigabit Ethernet to the appropriate PVC.

To configure the for PPPoE feature, you should understand the following concepts:

- [MAC Address for PPPoEoA, page 12](#)
- [Benefits of the Configurable MAC Address for PPPoE Feature, page 12](#)

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 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 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.

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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	bba-group pppoe { <i>bba-group-name</i> global } Example: Router(config)# bba-group pppoe group1	Enters BBA group configuration mode.
Step 4	mac-address { autoselect <i>mac-address</i> } Example: Router(config-bba-group)# mac-address autoselect	Selects the MAC address, as follows: <ul style="list-style-type: none"> autoselect—Automatically selects the MAC address based on the ATM interface address, plus 7. <i>mac-address</i>—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: Router(config-bba-group)# end	Exits BBA group configuration mode.
Step 6	show pppoe session Example: Router# show pppoe session	Displays the MAC address as the local MAC (LocMac) address on the last line of the display.

Examples

The following example shows the display of the MAC address as LocMac:

```
Router# show pppoe session

1 session in LOCALLY_TERMINATED (PTA) State
  1 session total

Uniq ID  PPPoE  RemMAC          Port          VT  VA
State
          SID  LocMAC
      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 router 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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	bba-group pppoe { <i>group-name</i> global } Example: Router(config)# bba-group pppoe global	Defines a PPPoE profile and enters BBA group configuration mode. <ul style="list-style-type: none"> • The global keyword creates a profile that will serve as the default profile for any PPPoE port that is not assigned a specific profile.

	Command or Action	Purpose
Step 4	sessions auto cleanup Example: Router(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: Router(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

Perform this task to monitor and maintain 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: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show pppoe session [all packets] Example: Router# show pppoe session all	Displays information about active PPPoE sessions.

	Command or Action	Purpose
Step 3	<pre>clear pppoe {interface type number [vc {[vpi/]vci vc-name}] rmac mac-addr [sid session-id] all}</pre> <p>Example: Router# clear pppoe interface atm 0/0/0.0</p>	Terminates PPPoE sessions.
Step 4	<pre>debug pppoe {data errors events packets} [rmac remote-mac-address interface type number [vc {[vpi/]vci vc-name}]}</pre> <p>Example: Router# debug pppoe events</p>	Displays debugging information for PPPoE sessions.

Configuration Examples for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

This section provides the following configuration examples:

- [PPPoE Profiles Configuration: Example, page 16](#)
- [MAC Address of the PPPoEoA Session as the Burned-In MAC Address: Example, page 18](#)
- [Address Autoselect Configured and MAC Address Not Configured: Example, page 18](#)
- [MAC Address Configured on the ATM Interface: Example, page 19](#)
- [MAC Address Configured on the BBA Group: Example, page 19](#)
- [PPPoE Session Recovery After Reload: Example, page 20](#)

PPPoE Profiles Configuration: Example

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 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
!
```

MAC Address of the PPPoEoA Session as the Burned-In MAC Address: Example

In the following example, neither address autoselect nor a MAC address is configured on the BBA group, and 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).
```

Address Autoselect Configured and MAC Address Not Configured: Example

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)
    
```

MAC Address Configured on the ATM Interface: Example

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).
    
```

MAC Address Configured on the BBA Group: Example

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)
```

PPPoE Session Recovery After Reload: Example

In the following example, the router will attempt to recover failed PPPoE sessions on PVCs in the ATM PVC range called “range-pppoe-1”.

```
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

The following sections provide references related to providing protocol support for broadband access aggregation of PPPoE sessions.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Broadband and DSL commands	Cisco IOS 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	Identifying a Physical Subscriber Line for RADIUS Access and Accounting
Configuring a Cisco Subscriber Service Switch	Configuring ISG Policies for Automatic Subscriber Logon

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1483	<i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i>
RFC 2516	<i>A Method for Transmitting PPP over Ethernet (PPPoE)</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 2 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. The following sections provide information about this feature: <ul style="list-style-type: none"> • “PPPoE Connection Throttling” section on page 3 • “Defining a PPPoE Profile” section on page 4
PPPoE Server Restructuring and PPPoE Profiles	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.



Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

First Published: March 14, 2011

Last Updated: March 14, 2011

PPP over ATM enables a high-capacity central site router with an ATM interface to terminate multiple remote PPP connections. PPP over ATM provides security validation per user, IP address pooling, and service selection capability.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions”](#) section on page 17.

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

Contents

- [Prerequisites for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions, page 2](#)
- [Restrictions for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions, page 2](#)
- [Information About Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions, page 2](#)
- [How to Provide Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions, page 3](#)
- [Configuration Examples for PPP over ATM, page 11](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Additional References](#), page 15
- [Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions](#), page 17

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](#), page 2

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 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, allowing each PPP connection to terminate at the router ATM interface as if received from a typical PPP serial interface.

The virtual access interface for each virtual circuit (VC) obtains its configuration from a virtual interface template (virtual template) when the VC is created. 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.

After you have configured the router for PPP over ATM, the PPP subsystem starts and the router 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.

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 two types of PPP over ATM connections are supported:

- IETF-compliant 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, page 3](#) (required)
- [Configuring IETF-Compliant MUX Encapsulated PPP over ATM on a Multipoint Subinterface, page 5](#) (required)
- [Configuring IETF-Compliant LLC Encapsulated PPP over ATM on a Point-to-point Subinterface, page 6](#) (required)
- [Configuring IETF-Compliant LLC Encapsulated PPP over ATM on a Multipoint Subinterface, page 9](#)(required)

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. **pvc** [*name*] *vpi/vci*
or
range [*range-name*] **pvc** *start-vpi/start-vci end-vpi/end-vci*
5. **encapsulation aal5mux ppp virtual-template** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>interface atm <i>number.subinterface-number</i> point-to-point</p> <p>Example: Router(config)# interface atm 1.0 point-to-point</p>	<p>Specifies the ATM point-to-point subinterface using the appropriate form of the interface atm command¹ and enters subinterface configuration mode.</p>
Step 4	<p>pvc [<i>name</i>] <i>vpi/vci</i> OR range [<i>range-name</i>] pvc <i>start-vpi/start-vci</i> <i>end-vpi/end-vci</i></p> <p>Example: Router(config-subif)# pvc cisco 0/5 OR Example: Router(config-subif)# range range1 pvc 1/200 1/299</p>	<p>Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.</p>
Step 5	<p>encapsulation aal5mux ppp virtual-template <i>number</i></p> <p>Example: Router(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3 OR Example: Router(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3</p>	<p>Configures VC multiplexed encapsulation on a PVC or PVC range.</p>
Step 6	<p>end</p> <p>Example: Router(config-subif-atm-vc)# end OR Example: Router(config-subif-atm-range)# end</p>	<p>Exits ATM virtual circuit range subinterface configuration mode. or Exits ATM range subinterface configuration mode.</p>

1. To determine the correct form of the **interface atm** command, consult your ATM shared port adapters documentation.

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 router. 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. **pvc** [*name*] *vpi/vci*
or
range [*range-name*] **pvc** *start-vpi/start-vci end-vpi/end-vci*
5. **encapsulation aal5mux ppp virtual-template** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface atm <i>number.subinterface-number</i> multipoint Example: Router(config)# interface atm 1/0/0.4 multipoint	Specifies the ATM multipoint subinterface using the appropriate form of the interface atm command ¹ and enters subinterface configuration mode.

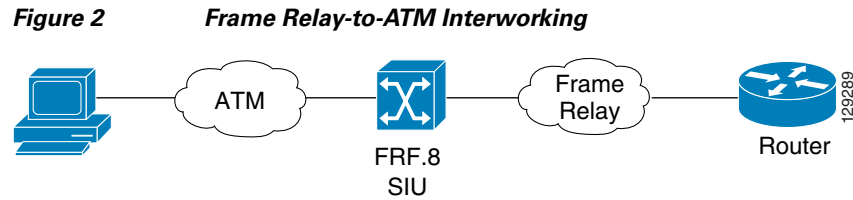
	Command or Action	Purpose
Step 4	<pre>pvc [name] vpi/vci or range [range-name] pvc start-vpi/start-vci end-vpi/end-vci</pre> <p>Example: Router(config-subif)# pvc cisco 0/5 or</p> <p>Example: Router(config-subif)# range range1 pvc 1/200 1/299</p>	Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.
Step 5	<pre>encapsulation aal5mux ppp virtual-template number</pre> <p>Example: Router(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3 or</p> <p>Example: Router(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3</p>	Configures VC multiplexed encapsulation on a PVC or PVC range.
Step 6	<pre>end</pre> <p>Example: Router(config-subif-atm-vc)# end or</p> <p>Example: Router(config-subif-atm-range)# end</p>	Exits ATM virtual circuit subinterface configuration mode. or Exits ATM range subinterface configuration mode.

- To determine the correct form of the **interface atm** command, consult your ATM shared port adapters documentation.

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.

Figure 2 shows 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. **pvc** [*name*] *vpi/vci*
or
range [*range-name*] **pvc** *start-vpi/end-vpi start-vci/end-vci*
5. **encapsulation aal15snap**
6. **protocol ppp virtual-template** *number*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>interface atm <i>number.subinterface-number</i> point-to-point</p> <p>Example: Router(config)# interface atm 6.200 point-to-point</p>	<p>Specifies the ATM point-to-point or multipoint subinterface using the appropriate form of the interface atm command¹ and enters subinterface configuration mode.</p>
Step 4	<p>pvc [<i>name</i>] <i>vpi/vci</i> OR range [<i>range-name</i>] pvc <i>start-vpi/start-vci</i> <i>end-vpi/end-vci</i></p> <p>Example: Router(config-subif)# pvc cisco 0/5 OR</p> <p>Example: Router(config-subif)# range range1 pvc 1/200 1/299</p>	<p>Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.</p>
Step 5	<p>encapsulation aal15snap</p> <p>Example: Router(config-subif-atm-vc)# encapsulation aal15snap OR</p> <p>Example: Router(config-subif-atm-range)# encapsulation aal15snap</p>	<p>Configures LLC SNAP encapsulation on the PVC or a range of PVCs.²</p>

	Command or Action	Purpose
Step 6	<p>protocol ppp virtual-template <i>number</i></p> <p>Example: Router(config-subif-atm-vc)# protocol ppp virtual-template 2 or</p> <p>Example: Router(config-subif-atm-range)# protocol ppp virtual-template 2</p>	Configures IETF PPP over ATM LLC encapsulation on the PVC or a range of PVCs.
Step 7	<p>end</p> <p>Example: Router(config-subif-atm-vc)# end or</p> <p>Example: Router(config-subif-atm-range)# end</p>	Exits ATM virtual circuit subinterface configuration mode. or Exits ATM range subinterface configuration mode.

1. To determine the correct form of the **interface atm** command, consult your ATM shared port adapters documentation.
2. “SNAP encapsulation” is a misnomer here, since this encapsulation configures both LLC and SNAP encapsulation on the VC. If SNAP encapsulation is not configured at a lower inheritance level, or another type of encapsulation is configured at a lower inheritance level, you will have to configure both SNAP and the **protocol ppp** command to ensure that PPP over ATM with LLC encapsulation is configured on your VC.

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 router.

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. **pvc** [*name*] *vpi/vci*
 or
range [*range-name*] **pvc** *start-vpi/end-vpi start-vci/end-vci*
5. **encapsulation aal15snap**
6. **protocol ppp virtual-template** *number*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>interface atm number.subinterface-number multipoint</p> <p>Example: Router(config)# interface atm 1/0/0.4 multipoint</p>	<p>Specifies the ATM multipoint subinterface using the appropriate form of the interface atm command¹ and enters subinterface configuration mode.</p>
Step 4	<p>pvc [name] vpi/vci OR range [range-name] pvc start-vpi/start-vci end-vpi/end-vci</p> <p>Example: Router(config-subif)# pvc cisco 0/5 OR</p> <p>Example: Router(config-subif)# range range1 pvc 1/200 1/299</p>	<p>Configures the PVC or a range of PVCs and enters ATM virtual circuit subinterface mode or ATM range subinterface configuration mode.</p>
Step 5	<p>encapsulation aal5mux ppp virtual-template number</p> <p>Example: Router(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3 OR</p> <p>Example: Router(config-subif-atm-range)# encapsulation aal5mux ppp virtual-template 3</p>	<p>Configures VC multiplexed encapsulation on a PVC or PVC range.</p>

	Command or Action	Purpose
Step 6	<pre>protocol ppp virtual-template number</pre> <p>Example: Router(config-subif-atm-vc)# protocol ppp virtual-template 2 or</p> <p>Example: Router(config-subif-atm-range)# protocol ppp virtual-template 2</p>	Configures IETF PPP over ATM LLC encapsulation on the PVC or a range of PVCs.
Step 7	<pre>end</pre> <p>Example: Router(config-subif-atm-vc)# end or</p> <p>Example: Router(config-subif-atm-range)# end</p>	Exits ATM virtual circuit subinterface configuration mode. or Exits ATM range subinterface configuration mode.

1. To determine the correct form of the **interface atm** command, consult your ATM shared port adapters documentation.

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

This section provides the following configuration examples:

- [IETF-Compliant MUX Encapsulated PPP over ATM Configuration, page 11](#)
- [IETF-Compliant LLC Encapsulated PPP over ATM Configuration, page 13](#)

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, page 11](#)
- [Example: Two Routers with Back-to-Back PVCs, page 12](#)
- [Example: Two Routers with Back-to-Back PVCs, page 12](#)
- [Example: Multiplexed Encapsulation Using VC Class, page 13](#)

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. For further information, see the [“Configuring IETF-Compliant MUX Encapsulated PPP over ATM on Point-to-Point Subinterface”](#) section on page 3.

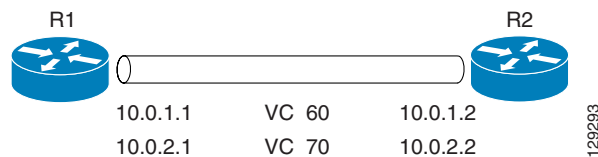
```
interface atm 2/0.1 multipoint
  pvc 0/60
    encapsulation aal5mux ppp virtual-template 3
    ubr 500
  exit

pvc 0/70
  encapsulation aal5mux ppp virtual-template 3
  vbr-nrt 1000 500 64
  exit
```

Example: Two Routers with Back-to-Back PVCs

Figure 3 illustrates an ATM interface with two PPP sessions over two PVC session connections. The sample commands following Figure 3 establish the back-to-back router configuration. For further information, see the [“Configuring IETF-Compliant MUX Encapsulated PPP over ATM on Point-to-Point Subinterface”](#) section on page 3.

Figure 3 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, page 13](#)
- [Example: Overriding a Virtual Template for IETF-Compliant PPP over ATM, page 14](#)
- [Example: Disabling IETF-Compliant PPP over ATM LLC Encapsulation on a Specific VC, page 14](#)

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. For further information, see the [“IETF-Compliant LLC Encapsulated PPP over ATM Configuration” section on page 13](#).

```
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, since the encapsulation option at that level is cisco ppp virtual template 1, as specified in the VC class called muxppp, the **protocol ppp virtual-template 2** command overrides only the virtual-template configuration. For further information, see the [“IETF-Compliant LLC Encapsulated PPP over ATM Configuration”](#) section on page 13.

```

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. For further information, see the [“IETF-Compliant LLC Encapsulated PPP over ATM Configuration”](#) section on page 13.

```

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	<i>Cisco IOS Master Commands List, All Releases</i>
Broadband and DSL commands	<i>Cisco IOS Broadband and DSL Command Reference</i>
Broadband access aggregation preparation tasks	<i>Preparing for Broadband Access Aggregation</i>
Configuring ATM	<i>Configuring ATM</i>

Standards

Standards	Title
Frame Relay Forum standard FRF.8	<i>Frame Relay to ATM Internetworking</i>

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 2364	<i>PPP over AAL5</i>

Technical Assistance

Description	Link
<p>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.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Table 5 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 5 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.

Table 5 *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	<p>PPP over ATM provides support for the termination of multiple PPP connections on an ATM interface of a router.</p> <p>In Cisco IOS XE Release 3.3S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • “Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions” section on page 17 • “Virtual Access Interface” section on page 2 • “How to Provide Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions” section on page 3 <p>The following commands were introduced or modified:</p> <p>encapsulation aal5mux ppp virtual-template, interface atm, protocol ppp virtual-template, pvc, range.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2011 Cisco Systems, Inc. All rights reserved.



PPPoE—QinQ Support

First Published: January 16, 2004
Last Updated: November 25, 2009

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.

Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE—QinQ Support](#)” section on [page 14](#).

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

Contents

- [Prerequisites for PPPoE—QinQ Support, page 2](#)
- [Information About PPPoE—QinQ Support, page 2](#)
- [How to Configure PPPoE—QinQ Support, page 5](#)
- [Configuration Examples for PPPoE—QinQ Support, page 10](#)
- [Additional References, page 12](#)
- [Feature Information for PPPoE—QinQ Support, page 14](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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

To configure the PPPoE—QinQ Support Feature, you should understand the following concepts:

- [PPPoE—QinQ Support on Subinterfaces, page 2](#)
- [Broadband Ethernet-Based DSLAM Model of QinQ VLANs, page 4](#)
- [Unambiguous and Ambiguous Subinterfaces, page 5](#)

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 [Figure 1 on page 3](#).

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.

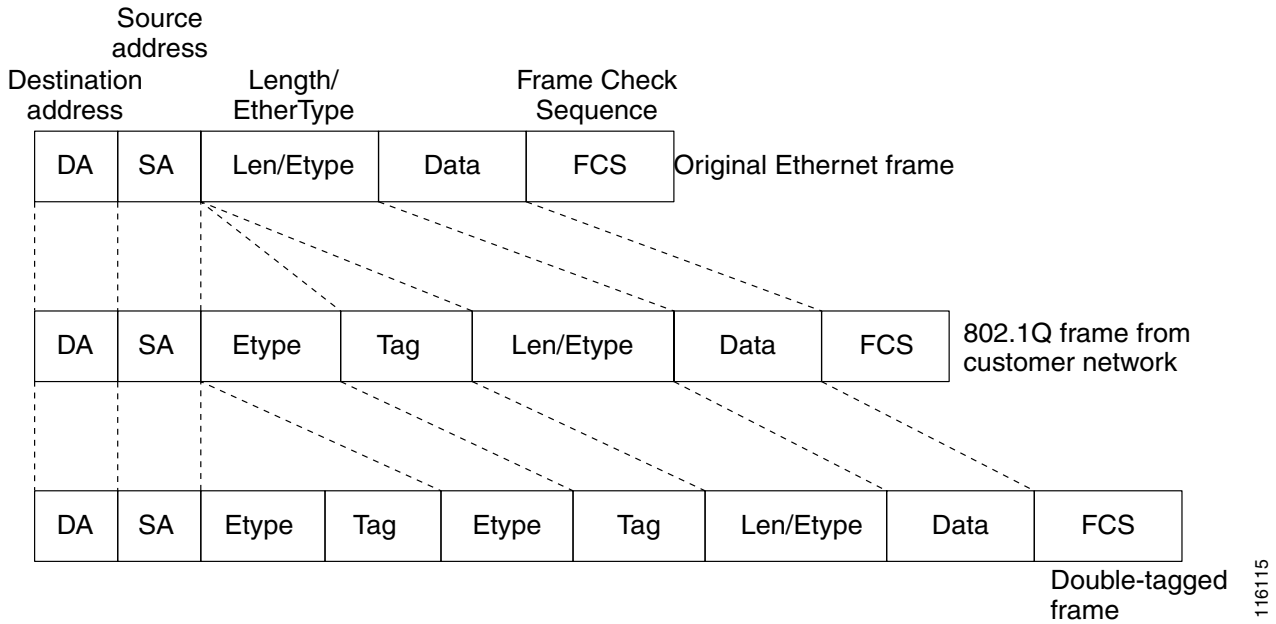
A primary consideration is whether you assign ambiguous or unambiguous subinterfaces for the inner VLAN ID. See the [“Unambiguous and Ambiguous Subinterfaces” section on page 5](#).

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 1 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames

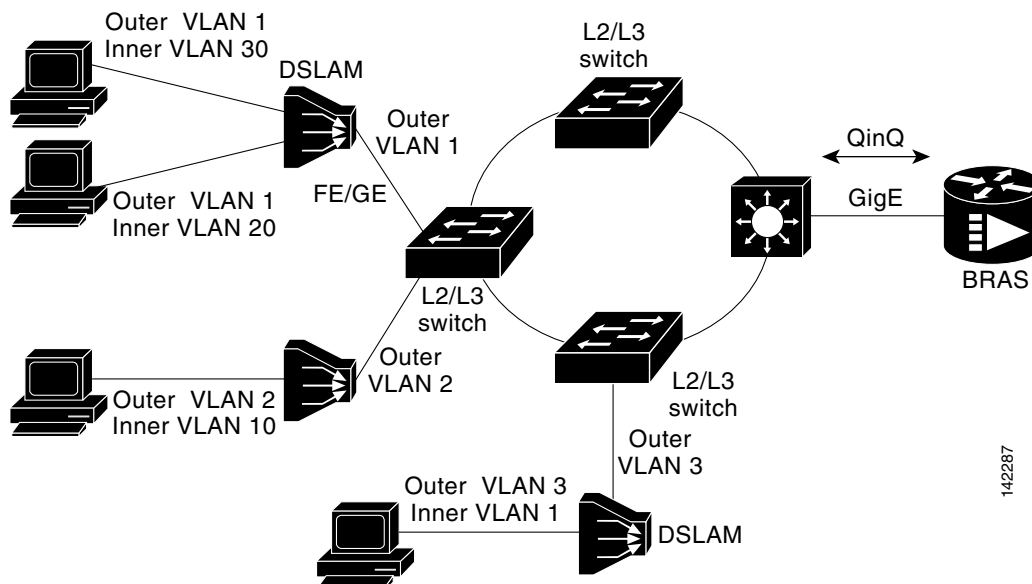


116115

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 [Figure 2](#), customers typically get their own VLAN; all these VLANs are aggregated on a DSLAM.

Figure 2 *Broadband Ethernet-Based DSLAM Model of QinQ VLANs*



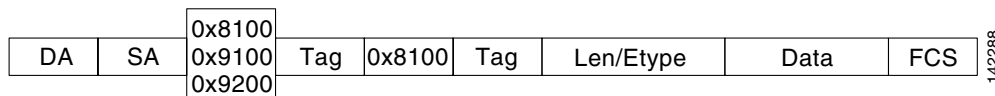
VLAN aggregation on a DSLAM will result in many aggregate VLANs that at some point need to be terminated on the broadband remote access servers (BRASs). Although the model could connect the DSLAMs directly to the BRAS, a more common model uses the existing Ethernet-switched network where each DSLAM VLAN 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. See [Figure 1](#).

QinQ encapsulation supports configurable outer tag Ethertype. The configurable Ethertype field values are 0x8100 (default), 0x9100, 0x9200, and 0x8848. See [Figure 3](#).

Figure 3 *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](#)” section on [page 10](#) 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

This section contains the following tasks:

- [Configuring the Interfaces for PPPoE—QinQ Support, page 5](#) (required)
- [Verifying the PPPoE—QinQ Support, page 8](#) (optional)

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.

Prerequisites



- 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, to enable PPPoE sessions or IP on the subinterface.
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/subslot/port</i> Example: Router(config)# interface gigabitethernet 1/0/0	Configures an interface and enters interface configuration mode.
Step 4	dot1q tunneling ethertype <i>ethertype</i> Example: Router(config-if)# dot1q tunneling ethertype 0x9100	(Optional) Defines the Ethertype field type used by peer devices when implementing QinQ VLAN tagging. <ul style="list-style-type: none">• Use this command if the Ethertype of peer devices is 0x9100 or 0x9200.

	Command or Action	Purpose
Step 5	<p>exit</p> <p>Example: Router(config-if)# exit</p>	Exits the interface configuration mode.
Step 6	<p>interface <i>type slot/subslot/port[.subinterface]</i></p> <p>Example: Router(config-if)# interface gigabitethernet 1/0/0.1</p>	Configures a subinterface and enters subinterface configuration mode.
Step 7	<p>encapsulation dot1q <i>vlan-id</i> second-dot1q {any <i>vlan-id</i> <i>vlan-id-vlan-id</i>[,<i>vlan-id-vlan-id</i>]}</p> <p>Example: Router(config-subif)# encapsulation dot1q 100 second-dot1q 200</p>	<p>(Required) Enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.</p> <ul style="list-style-type: none"> Use the second-dot1q keyword and the <i>vlan-id</i> 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	<p>pppoe enable [group <i>group-name</i>]</p> <p>Example: Router(config-subif)# pppoe enable group vpn1</p>	<p>(Optional) Enables PPPoE sessions on a subinterface.</p> <ul style="list-style-type: none"> The example specifies that the PPPoE profile, <i>vpn1</i>, will be used by PPPoE sessions on the subinterface. <p> Note This step is required only for PPPoEoQinQ.</p>
Step 9	<p>ip address <i>ip-address mask</i> [secondary]</p> <p>Example: Router(config-subif)# ip address 192.168.1.2 255.255.255.0</p>	<p>(Optional) Sets a primary or secondary IP address for a subinterface.</p> <ul style="list-style-type: none"> The example enables IP on the subinterface specified by the IP address, 192.168.1.2, and mask, 255.255.255.0. <p> Note This step is required only for IPoQinQ.</p>
Step 10	<p>exit</p> <p>Example: Router(config-subif)# exit</p>	Exits subinterface configuration mode.
Step 11	<p>Repeat Step 6 to configure another subinterface.</p> <p>Example: Router(config-if)# interface gigabitethernet 1/0/0.2</p>	(Optional) Configures a subinterface and enters subinterface configuration mode.

Command or Action	Purpose
<p>Step 12 Repeat Step 7, Step 8, and Step 9, as required, to specify the VLAN tags to be terminated on the subinterface.</p> <p>Example: <pre>Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600</pre></p> <p>Example: <pre>Router(config-subif)# pppoe enable group vpn1</pre></p> <p>Example: <pre>Router(config-subif)# ip address 192.168.1.2 255.255.255.0</pre></p>	<p>Specifies the VLAN tags to be terminated on the subinterface, to enable PPPoE sessions or IP on the subinterface.</p> <ul style="list-style-type: none"> Use the second-dot1q keyword and the <i>vlan-id</i> 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. 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. <p>Note Both PPPoE sessions and IP can be enabled on a subinterface.</p>
<p>Step 13 <code>end</code></p> <p>Example: <pre>Router(config-subif)# end</pre></p>	<p>Exits subinterface configuration mode and returns to privileged EXEC mode.</p>

Verifying the PPPoE—QinQ Support

Perform this optional task to verify the configuration of the PPPoE—QinQ Support feature.

SUMMARY STEPS

- enable**
- show running-config**
- 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.
- ```
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:

```
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.

```
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

This section provides the following example:

- [Configuring the any Keyword on Subinterfaces for PPPoE—QinQ Support: Example, page 10](#)

### 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

```

Table 1 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 1 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

```

Table 2 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 2** 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 |
| 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 | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a></li> <li><a href="#">Cisco IOS Master Command List, All Releases</a></li> </ul> |

## Standards

| Standards   | Title                                                         |
|-------------|---------------------------------------------------------------|
| IEEE 802.1Q | <i>IEEE Standard for Local and Metropolitan Area Networks</i> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                               | Title    |
|------------------------------------------------------------------------------------------------------------------------------------|----------|
| <p>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</p> | <p>—</p> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for PPPoE—QinQ Support

Table 3 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 3 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 3** 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.<br><br>Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">PPPoE—QinQ Support on Subinterfaces, page 2</a></li> </ul>                                                                                                      |
| PPPoE—QinQ Support                    | Cisco IOS XE Release 2.2 | This feature was introduced on Cisco ASR 1000 Series Routers.<br><br>This feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated. The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">How to Configure PPPoE—QinQ Support, page 5</a></li> </ul> The following commands were introduced or modified:<br><b>dot1q tunneling ethertype, encapsulation dot1q, show vlans dot1q.</b> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)



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

©2004–2009 Cisco Systems, Inc. All rights reserved.





# PPP-Max-Payload and IWF PPPoE Tag Support

---

**First Published: December 5, 2006**

**Last Updated: March 2, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPP-Max-Payload and IWF PPPoE Tag Support” section on page 9](#).

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

## Contents

- [Information About PPP-Max-Payload and IWF PPPoE Tag Support, page 2](#)
- [How to Configure PPP-Max-Payload and IWF PPPoE Tag Support, page 2](#)
- [Configuration Examples for PPP-Max Payload and IWF PPPoE Tag Support, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for PPP-Max-Payload and IWF PPPoE Tag Support, page 9](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Information About PPP-Max-Payload and IWF PPPoE Tag Support

To implement this feature, you should be familiar with the following concepts:

- [Accommodating an MTU/MRU Greater than 1492 in PPPoE](#)
- [Interworking Functionality](#)

## 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

This section contains the following tasks:

- [Enabling PPP-Max-Payload and IWF PPPoE Tag Support](#)
- [Disabling 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-name*
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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                   |
| Step 3 | <b>bba-group pppoe</b> { <i>group-name</i>   <b>global</b> }                                                          | Enters BBA group configuration mode and defines a PPPoE profile.                                                                                                                                                                                                                                    |
| Step 4 | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config-bba-group)# virtual-template 1 | Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. <ul style="list-style-type: none"> <li>• The <i>template-number</i> argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.</li> </ul> |

|         | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <p><b>tag ppp-max-payload</b> [minimum value maximum value] [deny]</p> <p><b>Example:</b><br/>Router(config-bba-group)# tag ppp-max-payload minimum 1200 maximum 3000</p>                          | <p>Specifies a range for the ppp-max payload tag value that will be accepted by the BRAS.</p> <ul style="list-style-type: none"> <li>• Default values are 1492 for the minimum and 1500 for the maximum.</li> <li>• The ppp-max-payload tag value accepted from the client cannot exceed the physical interface value for MTU minus 8.</li> </ul>                                                                                                                                                                                                                                                                                                 |
| Step 6  | <p><b>sessions per-mac iwf limit</b> per-mac-limit</p> <p><b>Example:</b><br/>Router(config-bba-group)# sessions per-mac iwf limit 200</p>                                                         | <p>Specifies a limit for IWF-specific sessions per MAC address (separate from session limits that are not IWF-specific).</p> <ul style="list-style-type: none"> <li>• If this command is not entered, the normal MAC-address session limit is applied to IWF sessions.</li> <li>• The <i>per-mac-limit</i> argument specifies the allowable number of IWF sessions. The default is 100.</li> </ul>                                                                                                                                                                                                                                                |
| Step 7  | <p><b>interface</b> {fastethernet   gigabitethernet   tengigabitethernet} slot/subslot/port[subinterface]</p> <p><b>Example:</b><br/>Router(config-bba-group)# interface gigabitethernet 0/0/0</p> | <p>Enters interface configuration mode for a Gigabit Ethernet interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 8  | <p><b>pppoe enable</b> [group group-name]</p> <p><b>Example:</b><br/>Router(config-if)# pppoe enable group 1</p>                                                                                   | <p>Enables PPPoE sessions on an Ethernet interface or subinterface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 9  | <p><b>virtual-template</b> template-number</p> <p><b>Example:</b><br/>Router(config-if)# virtual-template 1</p>                                                                                    | <p>Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.</p> <ul style="list-style-type: none"> <li>• The <i>template-number</i> argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 10 | <p><b>ppp lcp echo mru verify</b> [minimum value]</p> <p><b>Example:</b><br/>Router(config-if)# ppp lcp echo mru verify minimum 1304</p>                                                           | <p>Verifies the negotiated MRU and adjusts the PPP virtual access interface MTU for troubleshooting purposes.</p> <ul style="list-style-type: none"> <li>• If the optional <b>minimum</b> keyword is entered, the <i>value</i> can be from 64 to 1500.</li> <li>• 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.</li> </ul> |

|         | Command or Action                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-if)# end</code>                                        | Exits the current configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                         |
| Step 12 | <code>show pppoe session [all   packets]</code><br><br><b>Example:</b><br><code>Router# show pppoe session all</code> | Verifies the configuration and displays session information. <ul style="list-style-type: none"> <li><b>all</b>—Displays output indicating if a session is IWF-specific or if the PPP-Max-Payload tag is in the discovery frame and accepted.</li> <li><b>packets</b>—Displays packet statistics for the PPPoE session.</li> </ul> |

## 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 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code> | Enters interface configuration mode.                                                                             |

|        | Command or Action                                                     | Purpose                                                                                         |
|--------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Step 3 | <b>bba-group pppoe</b> { <i>group-name</i>   <b>global</b> }          | Enters BBA group configuration mode and defines a PPPoE profile.                                |
|        | <b>Example:</b><br>Router(config-if)# bba-group pppoe pppoe-group     |                                                                                                 |
| Step 4 | <b>tag ppp-max-payload deny</b>                                       | Disables the processing of the ppp-max-payload tag value higher than the default of 1492 bytes. |
|        | <b>Example:</b><br>Router(config-bba-group)# tag ppp-max-payload deny |                                                                                                 |

## 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, page 6](#)
- [PPP-Max-Payload and IWF PPPoE Tag Support Disabled: Example, page 6](#)

### 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 | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a></li> <li>• <a href="#">Cisco IOS Master Command List, All Releases</a></li> </ul> |

## Standards

| Standard                       | Title                                                       |
|--------------------------------|-------------------------------------------------------------|
| DSL Forum Technical Report 101 | <a href="#">Migration to Ethernet-Based DSL Aggregation</a> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs               | Title                                                               |
|--------------------|---------------------------------------------------------------------|
| RFC 2516           | <a href="#">A Method for Transmitting PPP Over Ethernet (PPPoE)</a> |
| Draft RFC document | <a href="#">Accommodating an MTU/MRU Greater than 1492 in PPPoE</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for PPP-Max-Payload and IWF PPPoE Tag Support

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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 | <p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>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.</p> <p>The following commands were introduced or modified: <b>ppp lcp echo mru verify, sessions per-mac iwf limit, show pppoe session, tag ppp-max-payload.</b></p> |

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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

© 2006–2009 Cisco Systems, Inc. All rights reserved.





# PPPoE Session Limiting on Inner QinQ VLAN

---

**First Published: December 4, 2006**

**Last Updated: November 25, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE Session Limiting on Inner QinQ VLAN” section on page 7](#).

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

## Contents

- [Prerequisites for PPPoE Session Limiting on Inner QinQ VLAN, page 2](#)
- [Restrictions for PPPoE Session Limiting on Inner QinQ VLAN, page 2](#)
- [Information About PPPoE Session Limiting on Inner QinQ VLAN, page 2](#)
- [How to Configure PPPoE Session Limiting on Inner QinQ VLAN, page 3](#)
- [Configuration Examples for PPPoE Session Limiting on Inner QinQ VLAN, page 4](#)
- [Additional References, page 5](#)
- [Feature Information for PPPoE Session Limiting on Inner QinQ VLAN, page 7](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

## 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

To configure the PPPoE Session Limiting on Inner QinQ VLAN feature, you should understand the following concepts:

- [Benefits of PPPoE Session Limiting on Inner QinQ VLAN, page 2](#)
- [Feature Design of PPPoE Session Limiting on Inner QinQ VLAN, page 2](#)

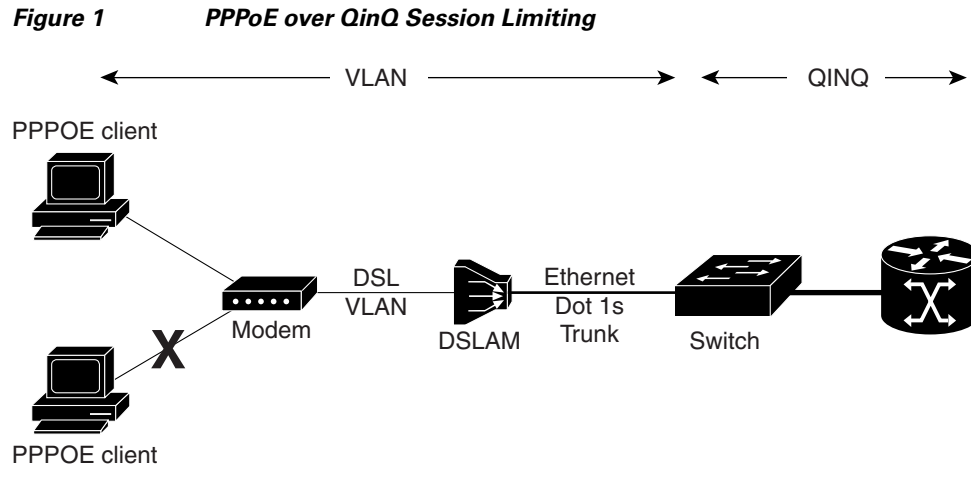
## Benefits of PPPoE Session Limiting on Inner QinQ VLAN

- 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.

[Figure 1](#) shows a typical implementation of the PPPoE Session Limiting on Inner QinQ VLAN feature.



180452

# How to Configure PPPoE Session Limiting on Inner QinQ VLAN

This section contains the following procedure:

- [Configuring PPPoE Session Limiting on Inner QinQ VLAN, page 3](#)

## 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 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code> | Enters global configuration mode.                                       |

|        | Command or Action                                                                                                                                                                              | Purpose                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 3 | <b>bba-group</b> <b>pppoe</b> <i>group-name</i><br><br><b>Example:</b><br>Router(config)# bba-group pppoe group 1                                                                              | Creates a PPPoE profile and enters the bba-group configuration mode.                 |
| Step 4 | <b>sessions per-vlan limit</b> <i>outer-per-vlan-limit</i><br><b>inner</b> <i>inner-per-vlan-limit</i><br><br><b>Example:</b><br>Router(config-bba-group)# sessions per-vlan-limit 400 inner 1 | Configures inner and outer VLAN limits.                                              |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>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

This section provides the following configuration example:

- [PPPoE Session Limiting on Inner QinQ VLAN: Example, page 4](#)

### 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 | <i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i> |
| Broadband access commands             | <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i>      |

## Standards

| Standard             | Title                                      |
|----------------------|--------------------------------------------|
| IEEE Standard 802.1Q | <i>Virtual Bridged Local Area Networks</i> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                    |
|----------|--------------------------|
| RFC 2516 | <i>PPP over Ethernet</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for PPPoE Session Limiting on Inner QinQ VLAN

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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.<br><br>The following command was modified by this feature:<br><b>session per-vlan limit.</b> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2006–2009 Cisco Systems, Inc. All rights reserved.





# PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

---

**First Published: January, 2005**  
**Last Updated: November 25, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement”](#) section on page 10.

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

## Contents

- [Prerequisites for the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement, page 2](#)
- [Information About the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement, page 2](#)
- [How to Configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement, page 4](#)
- [Configuration Examples for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement, page 7](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- [Additional References](#), page 8
- [Feature Information for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement](#), page 10
- [Glossary](#), page 11

## 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](#)” section on page 8 for more information.

## Information About the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

To configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature, you should understand the following concepts:

- [Differences Between ATM and Fast or Gigabit Ethernet-Based Broadband Access Networks](#), page 2
- [DSL Forum 2004-71: Solution for Remote-ID in PPPoE Discovery Phase](#), page 2
- [Remote-ID Tag in Fast or Gigabit Ethernet-Based Broadband Access Networks](#), page 3
- [Benefits of the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement](#), page 4

## 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

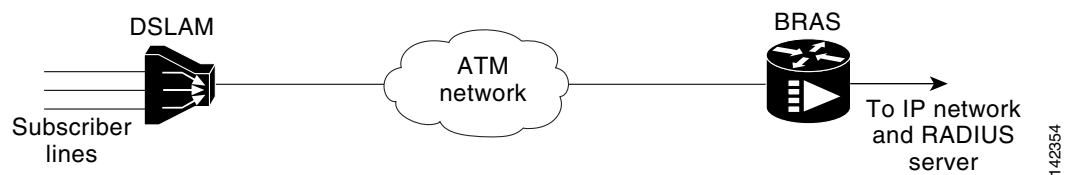
DSL Forum 2004-71 defines a method whereby the DSLAM sends the DSL Remote-ID tag in the PPP over Ethernet (PPPoE) discovery phase to apply the same subscriber mapping capability to Fast or Gigabit Ethernet interfaces that is possible on ATM interfaces. This method adds support for the PPPoE

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 [Figure 1-1](#).

**Figure 1-1** ATM-Based DSL Broadband Access Network

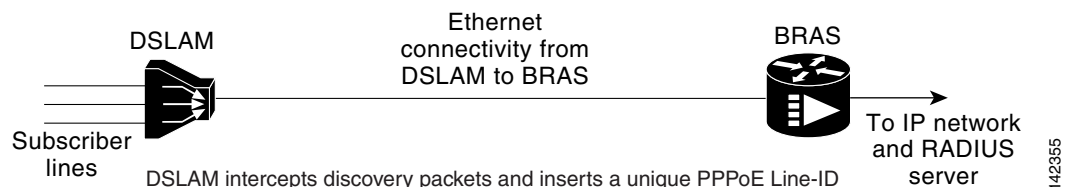


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM virtual circuit (VC) used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-ID tag for use in RADIUS packets.

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 [Figure 1-2](#). 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 1-2** PPPoE Remote-ID Tag Processing Solution



DSLAM intercepts discovery packets and inserts a unique PPPoE Line-ID tag to PADI or PADR packets and forwards upstream to BRAS.

BRAS processes the tag and extracts the Remote-ID, which is stored on the session.

The Remote-ID is sent as a NAS-Port-ID attribute in AAA accounting and PPP authentication requests.

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

This section contains the following procedures:

- [Configuring the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement Feature, page 4](#)
- [Stripping Vendor-Specific Tags, page 6](#)

## 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. **radius-server attribute 31 remote-id**
4. **bba-group pppoe *group-name***
5. **vendor-tag remote-id service**
6. **vendor-tag dsl-sync-rate service**
7. **nas-port-id format c**
8. **end**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                   | <b>Purpose</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>aaa new-model</b><br><br><b>Example:</b><br>Router(config)# <b>aaa new-model</b>                                        | (Optional) Enables the AAA access control model.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 4</b> | <b>radius-server attribute 31 remote-id</b><br><br><b>Example:</b><br>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. <ul style="list-style-type: none"> <li>• Configure this command so that the Acct-Session-ID attribute, as displayed in the <b>debug radius</b> command, will contain the information about the incoming access interface, where discovery frames are received, and about the session being established. See the <a href="#">“Troubleshooting Tips” section on page 7</a> section for more information that follows the <a href="#">“Stripping Vendor-Specific Tags”</a> task.</li> </ul> |
| <b>Step 5</b> | <b>bba-group pppoe <i>group-name</i></b><br><br><b>Example:</b><br>Router(config)# bba-group pppoe pppoe-group             | Defines a PPPoE profile and enters BBA group configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 6</b> | <b>vendor-tag remote-id service</b><br><br><b>Example:</b><br>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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>vendor-tag dsl-sync-rate service</b><br><br><b>Example:</b><br>Router(config-bba-group)# vendor-tag<br>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 | <b>nas-port-id format c</b><br><br><b>Example:</b><br>Router(config-bba-group)# nas-port-id format c                            | Specifies a format for broadband subscriber access line identification coding. <ul style="list-style-type: none"> <li>The designation of <b>format c</b> is specifically designed for a particular coding format. A sample of this format is as follows:<br/>               NAS_PORT_ID=atm 31/31/7:255.65535<br/>               example001/0/31/63/31/127</li> <li>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.<br/><br/>               The Circuit-ID/Remote-ID tag is<br/>               example001/0/31/63/31/127.</li> </ul> |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                  | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                          | Enters global configuration mode.                                                                                                                         |
| Step 3 | <b>bba-group pppoe group-name</b><br><br><b>Example:</b><br>Router(config)# bba-group pppoe pppoe-group | Defines a PPPoE profile and enters BBA group configuration mode.                                                                                          |
| Step 4 | <b>vendor-tag strip</b><br><br><b>Example:</b><br>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 | <b>end</b><br><br><b>Example:</b><br>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

This section contains the following examples:

- [Configuring PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement: Example, page 7](#)
- [Stripping Vendor-Specific Tags: Example, page 8](#)

## 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                               | <i>Cisco IOS XE Broadband and DSL Configuration Guide</i>                    |
| RADIUS attributes                                           | <a href="#">RADIUS Attributes Overview and RADIUS IETF Attributes</a> module |
| DSL Line-ID tag solution                                    | <a href="#">RFC 4679 - DSL Forum Vendor Specific RADIUS Attributes</a>       |
| Migration to Fast or Gigabit Ethernet-based DSL aggregation | <a href="#">DSL Forum Technical Report 101</a>                               |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                      |
|----------|------------------------------------------------------------|
| RFC 2516 | <i>A Method for Transmitting PPP over Ethernet (PPPoE)</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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. | <p>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.</p> <p>The following commands were introduced or modified:<br/> <b>radius-server attribute, bba-group pppoe group-name, vendor-tag remote-id service, vendor-tag dsl-sync-rate service, nas-port-id format c.</b></p> |

# 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005–2009 Cisco Systems, Inc. All rights reserved.



# Enabling PPPoE Relay Discovery and Service Selection Functionality

---

**First Published: May 2, 2005**  
**Last Updated: May 4, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for Enabling PPPoE Relay Discovery and Service Selection Functionality”](#) section on page 14.

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

## Contents

- [Prerequisites for Enabling PPPoE Relay Discovery and Service Selection Functionality, page 2](#)
- [Information About Enabling PPPoE Relay Discovery and Service Selection Functionality, page 2](#)
- [How to Enable PPPoE Relay Discovery and Service Selection Functionality, page 2](#)
- [Configuration Examples for Enabling PPPoE Relay Discovery and Service Selection Functionality, page 7](#)
- [Additional References, page 13](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2005–2009 Cisco Systems, Inc. All rights reserved.



- [Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality, page 14](#)

## 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. See the “[Related Documents](#)” section on [page 13](#) for more information about these features.

## Information About Enabling PPPoE Relay Discovery and Service Selection Functionality

To configure PPPoE relay, you need to understand the following concept:

- [L2TP Active Discovery Relay for PPPoE, page 2](#)

### 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). (See the “[RFCs](#)” section on [page 13](#) for information on how to access Network Working Group Internet-Drafts.)

The key benefit of the PPPoE Relay feature is end-to-end control of services between the LNS and a PPPoE client.

## How to Enable PPPoE Relay Discovery and Service Selection Functionality

This section contains the following procedures:

- [Configuring the LAC and Tunnel Switch for PPPoE Relay, page 3](#) (required)
- [Configuring the LNS \(or Multihop Node\) to Respond to Relayed PAD Messages, page 4](#) (required)

- [Additional References, page 13](#) (optional)

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>subscriber profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config)# subscriber profile profile-1 | Configures the subscriber profile name and enters subscriber profile configuration mode. <ul style="list-style-type: none"> <li>• <i>profile-name</i>—Is referenced from a PPPoE profile configured by the <b>bba-group pppoe</b> global configuration command, so that all the PPPoE sessions using the PPPoE profile defined by the <b>bba-group pppoe</b> command will be treated according to the defined subscriber profile.</li> </ul> |

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>service relay pppoe vpdn group</b> <i>vpdn-group-name</i><br><br><b>Example:</b><br>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. <ul style="list-style-type: none"> <li>See the <a href="#">“The following example shows how to enter Subscriber Service Switch subscriber service attributes in a AAA RADIUS server profile.”</a> section for the equivalent RADIUS profile entry.</li> </ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>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 [“Configuring the LNS \(or Multihop Node\) to Respond to Relayed PAD Messages”](#) 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

- enable**
- configure terminal**
- vpdn-group** *vpdn-group-name*
- accept-dialin**
- protocol l2tp**
- virtual-template** *template-number*
- exit**
- terminate-from hostname** *host-name*
- relay pppoe bba-group** *pppoe-bba-group-name*
- exit**

## DETAILED STEPS

|        | Command or Action                                                                                                            | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                               | Enters global configuration mode.                                                                                |
| Step 3 | <b>vpdn-group</b> <i>vpdn-group-name</i><br><br><b>Example:</b><br>Router(config)# vpdn-group Group-A                        | Creates a VPDN group and enters VPDN group configuration mode.                                                   |
| Step 4 | <b>accept-dialin</b><br><br><b>Example:</b><br>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 | <b>protocol l2tp</b><br><br><b>Example:</b><br>Router(config-vpdn-req-in)# protocol l2tp                                     | Specifies the L2TP tunneling protocol.                                                                           |
| Step 6 | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config-vpdn-req-in)# virtual-template 2      | Specifies which virtual template will be used to clone virtual access interfaces.                                |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vpdn-req-in)# exit                                                       | Exits to VPDN group configuration mode.                                                                          |
| Step 8 | <b>terminate-from hostname</b> <i>host-name</i><br><br><b>Example:</b><br>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  | <pre>relay pppoe bba-group pppoe-bba-group-name</pre> <p><b>Example:</b><br/>Router(config-vpdn)# relay pppoe bba-group group-2</p> | <p>Specifies the PPPoE BBA group that will respond to the PAD messages.</p> <ul style="list-style-type: none"> <li>The PPPoE BBA group name is defined with the <b>bba-group pppoe group-name</b> global configuration command.</li> <li>See the “<a href="#">RADIUS VPDN Group User Profile Entry for the LNS</a>” section for the equivalent RADIUS profile entry.</li> </ul> |
| Step 10 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vpdn)# exit</p>                                                                | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                      |

## Monitoring PPPoE Relay

Perform this task to monitor PPPoE Relay.

### SUMMARY STEPS

- enable
- show pppoe session
- show pppoe relay context all
- clear pppoe relay context

### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                                 |
|--------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                      | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <pre>show pppoe session</pre> <p><b>Example:</b><br/>Router# show pppoe session</p> | <p>Displays information about currently active PPPoE sessions.</p>                                                      |

#### Step 1 enable

Enables privileged EXEC mode.

- Enter your password if prompted.

Router> **enable**

#### Step 2 show pppoe session

Displays information about currently active PPPoE sessions.

**Router# show pppoe session**

```

1 session in FORWARDED (FWDED) State
1 session total

Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC
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.

```

Router# show pppoe relay context all

Total PPPoE relay contexts 1
UID ID Subscriber-profile State
25 18 cisco.com RELAYED

```

**Step 4 clear pppoe relay context**

This command clears the PPPoE relay context created for relaying PAD messages.

```

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

This section provides the following configuration examples:

- [PPPoE Relay on LAC Configuration: Example, page 8](#)
- [Basic LNS Configured for PPPoE Relay: Example, page 8](#)
- [Tunnel Switch \(or Multihop Node\) Configured to Respond to PAD Messages: Example, page 10](#)
- [Tunnel Switch Configured to Relay PAD Messages: Example, page 11](#)
- [RADIUS Subscriber Profile Entry for the LAC: Example, page 12](#)
- [RADIUS VPDN Group User Profile Entry for the LNS: Example, page 12](#)

## 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 msgbpgroup 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                                         | <i>Cisco IOS XE Dial Technologies Configuration Guide</i>                    |
| VPDN tunnel commands                                 | <i>Cisco IOS XE Dial Technologies Configuration Guide</i>                    |
| Tunnel switching                                     | <i>L2TP Tunnel Switching</i> feature module                                  |
| PPPoE broadband groups                               | <i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i> |
| PPPoE broadband commands                             | <i>Cisco IOS XE Broadband Access Aggregation and DSL Command Reference</i>   |
| Broadband access aggregation concepts                | <i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i> |
| Tasks for preparing for broadband access aggregation | <i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                                                                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RFC 2516 | <i>Method for Transmitting PPP Over Ethernet (PPPoE)</i>                                                                                                                                                                                                                                                                                           |
| RFC 3817 | <ul style="list-style-type: none"> <li><i>L2TP Active Discovery Relay for PPPoE</i></li> <li>Network Working Group Internet-Draft, <i>L2TP Active Discovery Relay for PPPoE</i>, which can be seen at <a href="http://tools.ietf.org/html/draft-dasilva-l2tp-relaysvc-06">http://tools.ietf.org/html/draft-dasilva-l2tp-relaysvc-06</a></li> </ul> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

Table 10 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 10 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 10** 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 | <p>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).</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>“<a href="#">Information About Enabling PPPoE Relay Discovery and Service Selection Functionality</a>” section on page 2</li> <li>“<a href="#">How to Enable PPPoE Relay Discovery and Service Selection Functionality</a>” section on page 2</li> </ul> <p>This feature was integrated into Cisco IOS XE Release 2.1.</p> |
| PPPoE Service Selection | Cisco IOS XE Release 2.4 | This feature was integrated into Cisco IOS XE Release 2.4.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2005–2009 Cisco Systems, Inc. All rights reserved.





# Configuring Cisco Subscriber Service Switch Policies

---

**First Published: May 2, 2005**  
**Last Updated: May 4, 2009**

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 determine 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.

## Finding Feature Information in This Module

For the latest feature information and caveats, see 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 for Configuring a Subscriber Service Switch Policy” section on page 28](#).

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

## Contents

- [Prerequisites for Configuring a Subscriber Service Switch Policy, page 2](#)
- [Restrictions for Configuring a Subscriber Service Switch Policy, page 2](#)
- [Information About the Subscriber Service Switch, page 2](#)
- [How to Configure a Subscriber Service Switch Policy, page 5](#)
- [Configuration Examples for Configuring a Subscriber Service Switch Policy, page 11](#)
- [Where to Go Next, page 27](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**



- [Additional References, page 27](#)
- [Feature Information for Configuring a Subscriber Service Switch Policy, page 28](#)

## 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.

To configure the Cisco Subscriber Server Switch policy, you should understand the following concepts:

- [Benefits of the Subscriber Service Switch, page 2](#)
- [Backward Compatibility of Subscriber Service Switch Policies, page 3](#)

## Benefits of the Subscriber Service Switch

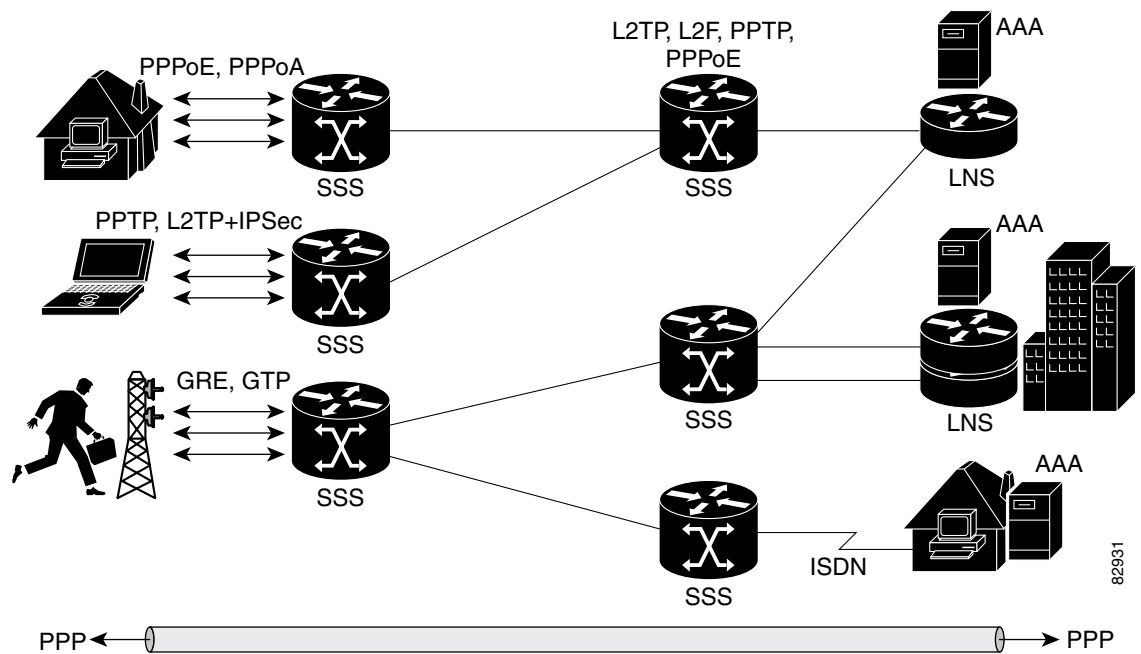
The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determine which services to provide to subscribers, the number of subscribers, 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).

Figure 1 shows how the Subscriber Service Switch provides its own centralized switching path that bypasses the virtual-access-based switching available earlier. In Figure 1, the Subscriber Service Switch is switching data traffic from personal computers in a home and corporate office and from a wireless user.

**Figure 1 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:
  1. Authorization for VPDN call termination (using the **accept-dialin** and **accept-dialout** keywords).
  2. Authorization for VPDN subscriber service (using the **request-dialin** and **request-dialout** keywords).
  3. A directive to collect further service keys and reauthorize (using the **authen-before-forward** keyword).
  4. 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.

## 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.

This section contains the following procedures:

- [Enabling Domain Preauthorization on a NAS, page 5](#) (required)
- [Creating a RADIUS User Profile for Domain Preauthorization, page 6](#) (required)
- [Enabling a Subscriber Service Switch Preauthorization, page 7](#) (required)
- [Troubleshooting the Subscriber Service Switch, page 8](#) (optional)

### 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. **show running-config**

## DETAILED STEPS

|        | Command or Action                                                                            | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal               | Enters global configuration mode.                                                                                |
| Step 3 | <b>vpdn authorize domain</b><br><br><b>Example:</b><br>Router(config)# vpdn authorize domain | Enables domain preauthorization on an Network Access Server (NAS).                                               |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                   | Exits global configuration mode.                                                                                 |
| Step 5 | <b>show running-config</b><br><br><b>Example:</b><br>Router# 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 [“Creating a RADIUS User Profile for Domain Preauthorization”](#) section on page 6 for more information.

## Creating a RADIUS User Profile for Domain Preauthorization

Table 1 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 1** Attributes for the RADIUS User Profile for Domain Preauthorization

| RADIUS Entry                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>nas-port:</b> <i>ip-address:slot/subslot/port/vpi.vci</i> | Configures the NAS port username for domain preauthorization. <ul style="list-style-type: none"> <li><i>ip-address</i>:—Management IP address of the node switch processor (NSP).</li> <li><i>slot/subslot/port</i>:—Specifies the ATM interface.</li> <li><i>vpi.vci</i>:—Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.</li> </ul> |
| <b>Password=</b> “cisco”                                     | Sets the fixed password.                                                                                                                                                                                                                                                                                                                                                     |

| RADIUS Entry                                              | Purpose                                                                                                                                               |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. <ul style="list-style-type: none"> <li>domain—Domain to configure as accessible to the user.</li> </ul> |

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>subscriber access {pppoe   pppoa} pre-authorize nas-port-id [aaa-method-list]</b><br><br><b>Example:</b><br>Router(config)# subscriber access pppoe pre-authorize nas-port-id mlist-llid | Enables Subscriber Service Switch preauthorization. <p><b>Note</b> 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.</p> |

|        | Command or Action                                                                            | Purpose                                                |
|--------|----------------------------------------------------------------------------------------------|--------------------------------------------------------|
| Step 4 | <b>show sss session [all]</b><br><br><b>Example:</b><br>Router(config)# show sss session all | Displays the Subscriber Service Switch session status. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>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 [“Troubleshooting the Subscriber Service Switch”](#) section on page 8.

## 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”](#) section on page 14. Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

## 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. Table 2 lists some of these **debug** commands.

**Table 2** Additional Debugging Commands for Troubleshooting the Subscriber Service Switch

| Command                       | Purpose                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>debug ppp negotiation</b>  | Allows you to check that a client is passing PPP negotiation information.                                     |
| <b>debug pppoe errors</b>     | Displays PPPoE error messages.                                                                                |
| <b>debug pppoe events</b>     | Displays protocol event information.                                                                          |
| <b>debug vpdn call events</b> | Enables VPDN call event debugging.                                                                            |
| <b>debug vpdn call fsm</b>    | Enables VPDN call setup state debugging.                                                                      |
| <b>debug vpdn elog</b>        | Enables VPDN performance event data collection.                                                               |
| <b>debug vpdn events</b>      | Displays PPTP tunnel event change information.                                                                |
| <b>debug vpdn l2x-data</b>    | Enables L2F and L2TP event and data debugging.                                                                |
| <b>debug vpdn l2x-errors</b>  | Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.                  |
| <b>debug vpdn l2x-events</b>  | Displays L2F and L2TP events that are part of tunnel establishment or shutdown.                               |
| <b>debug vpdn l2x-packets</b> | Enables L2F and L2TP packet level debugging.                                                                  |
| <b>debug vpdn errors</b>      | Displays PPTP protocol error messages.                                                                        |
| <b>debug vpdn message</b>     | Enables VPDN inter processing message debugging.                                                              |
| <b>debug vpdn packet</b>      | Enables VPDN packet level debugging.                                                                          |
| <b>debug vpdn scalability</b> | Enables VPDN scalability debugging.                                                                           |
| <b>debug vpdn sss errors</b>  | Displays diagnostic information about errors that may occur during VPDN Subscriber Service Switch call setup. |
| <b>debug vpdn sss events</b>  | 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.

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 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                          |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <code>no logging console</code><br><br><b>Example:</b><br>Router(config)# <code>no logging console</code> | Disables all logging to the console terminal. <ul style="list-style-type: none"> <li>To reenable logging to the console, use the <b>logging console</b> command.</li> </ul>                                                                                                                                                                                                                                               |
| 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 | <code>terminal monitor</code><br><br><b>Example:</b><br>Router(config)# <code>terminal monitor</code>     | Enables logging output on the virtual terminal.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 6 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# <code>exit</code>                             | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 7 | <code>debug sss command-option</code><br><br><b>Example:</b><br>Router# <code>debug sss error</code>      | Enables the <b>debug</b> command. <ul style="list-style-type: none"> <li>See the “<a href="#">Debug Commands Available for Subscriber Service Switch</a>” section on page 8 and the “<a href="#">Additional Debugging Commands for Troubleshooting the Subscriber Service Switch</a>” section on page 9 for commands that can be entered.</li> </ul> <p><b>Note</b> You can enter more than one <b>debug</b> command.</p> |
| Step 8 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                              | Purpose                                   |
|---------|------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 9  | <code>no terminal monitor</code><br><br><b>Example:</b><br>Router(config)# no terminal monitor | Disables logging on the virtual terminal. |
| Step 10 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# exit                               | Exits to privileged EXEC mode.            |

## Configuration Examples for Configuring a Subscriber Service Switch Policy

This section provides the following configuration examples:

- [LAC Domain Authorization: Example, page 11](#)
- [Domain Preauthorization RADIUS User Profile: Example, page 11](#)
- [Subscriber Service Switch Preauthorization: Example, page 12](#)
- [Verify Subscriber Service Switch Call Operation: Example, page 12](#)
- [Troubleshooting the Subscriber Service Switch Operation: Example, page 15](#)

### 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:

- [Troubleshooting the Subscriber Service Switch Operation: Example, page 15](#)
- [Troubleshooting the Subscriber Service Switch on the LAC—Normal Operation: Example, page 16](#)
- [Troubleshooting the Subscriber Service Switch on the LAC—Authorization Failure: Example, page 18](#)
- [Troubleshooting the Subscriber Service Switch on the LAC—Authentication Failure: Example, page 20](#)
- [Troubleshooting the Subscriber Service Switch on the LNS—Normal Operation: Example, page 23](#)
- [Troubleshooting the Subscriber Service Switch on the LNS—Tunnel Failure: Example, page 25](#)

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 : encaps 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_attr
*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_attr
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attr
*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_DISCNECT
*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 : encaps 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, c1
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                                                                                       | <a href="#">Understanding Broadband Access Aggregation</a> module                                    |
| Tasks for preparing for broadband access aggregation.                                                                       | <a href="#">Preparing for Broadband Access Aggregation</a> module                                    |
| Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | <a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a>                     |
| Configuration procedure for PPPoE.                                                                                          | <a href="#">Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions</a>        |
| Configuration procedures for PPPoA.                                                                                         | <a href="#">Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions</a> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                                                                        |
|----------|------------------------------------------------------------------------------|
| RFC 2661 | <i>Layer Two Tunneling Protocol L2TP</i>                                     |
| RFC 2341 | <i>Cisco Layer Two Forwarding (Protocol) L2F</i>                             |
| RFC 2516 | <i>A Method for Transmitting PPP Over Ethernet (PPPoE) (PPPoE Discovery)</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Configuring a Subscriber Service Switch Policy

Table 3 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 3 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 3** 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.<br><br>This feature was integrated into Cisco IOS XE Release 2.1. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2005–2009 Cisco Systems, Inc. All rights reserved.





# Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

---

**First Published: June 2003**  
**Last Updated: May 4, 2009**

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.

## Finding Feature Information in This Module

For the latest feature information and caveats, see 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 for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS”](#) section on page 15.

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

## Contents

- [Restrictions for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS, page 2](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2003–2009 Cisco Systems, Inc. All rights reserved.

- [Information About Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS](#), page 3
- [How to Use the Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS Feature](#), page 5
- [Configuration Examples for Per Session Queueing and Shaping Policies](#), page 10
- [Feature Information for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS](#), page 15

## 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, page 3](#)
- [How RADIUS Uses VSA 38 in User Profiles, page 3](#)
- [Commands Used to Define QoS Actions, page 4](#)

## 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” section on page 3](#) 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

The following sections contain procedures for configuring per session queueing and shaping:

- [Configuring a Per Session Queueing and Shaping Policy on the Router, page 5](#) (Required)
- [Verifying Per Session Queueing, page 10](#) (Required)

### 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 | <p><code>policy-map policy-map-name</code></p> <p><b>Example:</b><br/> Router(config)# <code>policy-map policy-map-name</code></p> | <p>Creates or modifies the bottom-level child policy.</p> <ul style="list-style-type: none"> <li><code>policy-map-name</code> is the name of the child policy map. The name can be a maximum of 40 alphanumeric characters.</li> </ul>                                                                                                                                                                         |
| Step 2 | <p><code>class</code></p> <p><b>Example:</b><br/> Router(config-pmap)# <code>class class-map-name</code></p>                       | <p>Assigns the traffic class you specify to the policy map.<br/> Enters policy-map class configuration mode.</p> <ul style="list-style-type: none"> <li><code>class-map-name</code> is the name of a previously configured class map and is the traffic class for which you want to define QoS actions.</li> <li>Repeat Steps 2 and 3 for each traffic class you want to include in the policy map.</li> </ul> |

| Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 3</b></p> <pre>bandwidth {bandwidth-kbps   percent percentage   remaining percent percentage} account {{qinq   dot1q} {aal5   aal3} {subscriber-encapsulation}}   {user-defined offset [atm]}}</pre> <p><b>Example:</b></p> <pre>Router(config-pmap-c)# bandwidth {bandwidth-kbps   percent percentage   remaining percent percentage} account {{qinq   dot1q} {aal5   aal3} subscriber-encapsulation   user-defined offset [atm]}</pre> | <p>Enables class-based fair queueing.</p> <ul style="list-style-type: none"> <li><i>bandwidth-kbps</i> 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.</li> <li><i>percent percentage</i> 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.</li> <li><i>remaining percent percentage</i> 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.</li> <li><b>account</b> enables ATM overhead accounting. For more information, see the “<a href="#">ATM Overhead Accounting</a>” section of the <i>Cisco 10000 Series Router Quality of Service Configuration Guide</i>, Chapter 15, “Configuring Dynamic Subscriber Services,” <a href="http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qrad.html#wp1067156">http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qrad.html#wp1067156</a>.</li> <li><b>qinq</b> specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type.</li> <li><b>dot1q</b> specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type.</li> <li><b>aal5</b> specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. You must specify either <b>aal5</b> or <b>aal3</b>.</li> <li><b>aal3</b> specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either <b>aal3</b> or <b>aal5</b>.</li> <li><i>subscriber-encapsulation</i> specifies the encapsulation type at the subscriber line.</li> <li><b>user-defined</b> indicates that the router is to use the <i>offset</i> you specify when calculating ATM overhead.</li> <li><i>offset</i> specifies the offset size the router is to use when calculating ATM overhead. Valid values are from –63 to 63 bytes.</li> </ul> <p><b>Note</b> The router configures the offset size if you do not specify the <i>offset</i> option.</p> <ul style="list-style-type: none"> <li><b>atm</b> applies ATM cell tax in the ATM overhead calculation.</li> </ul> <p><b>Note</b> Configuring both the <i>offset</i> and <b>atm</b> options adjusts the packet size to the offset size and then adds ATM cell tax.</p> |

|        | Command or Action                                                                                                  | Purpose                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap-c)# exit                                                  | Exits policy-map class configuration mode.                                                                                                                                                                       |
| Step 5 | <b>policy-map</b> <i>policy-map-name</i><br><br><b>Example:</b><br>Router(config-pmap)# policy-map policy-map-name | Creates or modifies the parent policy. <ul style="list-style-type: none"> <li>• <i>policy-map-name</i> is the name of the parent policy map. The name can be a maximum of 40 alphanumeric characters.</li> </ul> |
| Step 6 | <b>class</b> <b>class-default</b><br><br><b>Example:</b><br>Router(config-pmap)# class class-default               | Configures or modifies the parent class-default class.<br><br><b>Note</b> You can configure only the class-default class in a parent policy. Do not configure any other traffic class.                           |

| Command or Action                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 7</b></p> <pre>shape rate account {{{qinq   dot1q} {aal5   aal3} {subscriber-encapsulation}}   {user-defined offset [atm]}}</pre> <p><b>Example:</b></p> <pre>Router(config-pmap-c)# shape rate account {qinq   dot1q} {aal5   aal3} subscriber-encapsulation   {user-defined offset [atm]}</pre> | <p>Shapes traffic to the indicated bit rate and enables ATM overhead accounting.</p> <ul style="list-style-type: none"> <li>• <i>rate</i> is the bit-rate used to shape the traffic, expressed in kilobits per second.</li> <li>• <b>account</b> enables ATM overhead accounting.</li> <li>• <b>qinq</b> specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type.</li> <li>• <b>dot1q</b> specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type.</li> <li>• <b>aal5</b> specifies the ATM Adaptation Layer 5 that supports connection-oriented VBR services. You must specify either <b>aal5</b> or <b>aal3</b>.</li> <li>• <b>aal3</b> specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either <b>aal3</b> or <b>aal5</b>.</li> <li>• <i>subscriber-encapsulation</i> specifies the encapsulation type at the subscriber line.</li> <li>• <b>user-defined</b> indicates that the router is to use the <i>offset</i> you specify when calculating ATM overhead.</li> <li>• <i>offset</i> specifies the offset size the router is to use when calculating ATM overhead. Valid values are from -63 to 63 bytes.</li> </ul> <p><b>Note</b> The router configures the offset size if you do not specify the <b>user-defined</b> <i>offset</i> option.</p> <ul style="list-style-type: none"> <li>• <b>atm</b> applies ATM cell tax in the ATM overhead calculation.</li> </ul> <p>Configuring both the <i>offset</i> and <b>atm</b> options adjusts the packet size to the offset size and then adds ATM cell tax.</p> |
| <p><b>Step 8</b></p> <pre>service-policy policy-map-name</pre> <p><b>Example:</b></p> <pre>Router(config-pmap-c)# service-policy policy-map-name</pre>                                                                                                                                                       | <p>Applies a bottom-level child policy to the top-level parent class-default class.</p> <ul style="list-style-type: none"> <li>• <i>policy-map-name</i> is the name of the previously configured child policy map.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## 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# <b>show policy-map interface</b> <i>interface</i>    | 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. <ul style="list-style-type: none"> <li><i>interface</i> specifies the virtual-access interface and number the router created for the session (for example, virtual-access 1).</li> </ul> |
| Router# <b>show policy-map session uid</b> <i>uid-number</i> | Displays the session QoS counters for the subscriber session you specify. <ul style="list-style-type: none"> <li><b>uid</b> <i>uid-number</i> defines a unique session ID. Valid values for <i>uid-number</i> are from 1 to 65535.</li> </ul>                                                                                                                                                |
| Router# <b>show running-config</b>                           | 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

This section provides the following configuration examples:

- [Configuring a Per Session Queueing and Shaping Policy on the Router: Example, page 10](#)
- [Setting Up RADIUS for Per Session Queueing and Shaping: Example, page 11](#)
- [Verifying Per Session Queueing and Shaping Policies: Examples, page 11](#)

### 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 enables ATM overhead accounting.

```
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 aa15 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. In the example, overhead accounting is enabled for both shaping and bandwidth.

```

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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                         | Title |
|---------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported, and support for existing RFCs has not been modified. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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.<br><br>This feature was integrated into Cisco IOS XE Release 2.1. |

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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.

© 2003–2009 Cisco Systems, Inc. All rights reserved.





# 802.1P CoS Bit Set for PPP and PPPoE Control Frames

---

**First Published: December 4, 2006**  
**Last Updated: November 25, 2009**

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.

## Finding Feature Information in This Module

For the latest feature information and caveats, see 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 for 802.1P CoS Bit Set for PPP and PPPoE Control Frames”](#) section on page 7.

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

## Contents

- [Prerequisites for 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 2](#)
- [Restrictions for 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 2](#)
- [Information About 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 2](#)
- [How to Configure 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 3](#)
- [Configuration Examples for 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 3](#)
- [Additional References, page 5](#)
- [Feature Information for 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 7](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## 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:

- [Benefits of 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 2](#)
- [Feature Design of 802.1P CoS Bit Set for PPP and PPPoE Control Frames, page 2](#)

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, page 3](#)

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                  |
| Step 3 | <b>bba-group pppoe</b> <i>group-name</i><br><br><b>Example:</b><br>Router(config)# bba-group pppoe global                         | Specifies the BBA group and enters BBA group configuration mode.                                                   |
| Step 4 | <b>control-packets vlan cos</b> <i>priority</i><br><br><b>Example:</b><br>Router(config-bba-group)# control-packets vlan<br>cos 5 | Sets the PPPoE control packets associated with the BBA group.                                                      |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-bba-group)# exit                                                              | Exits BBA group configuration mode, and returns to global configuration mode.                                      |
| Step 6 | <b>bba-group pppoe</b> <i>group-name</i><br><br><b>Example:</b><br>Router(config)# bba-group pppoe cisco                          | Specifies the BBA group cisco and enters BBA group configuration mode.                                             |
| Step 7 | <b>control-packets vlan cos</b> <i>priority</i><br><br><b>Example:</b><br>Router(config-bba-group)# control-packets vlan<br>cos 2 | Sets the PPPoE control packets associated with the BBA group.                                                      |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>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 | <i>Cisco IOS XE Broadband and DSL Configuration Guide</i>               |
| Broadband access commands             | <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i> |

### Standards

| Standard             | Title                                      |
|----------------------|--------------------------------------------|
| IEEE Standard 802.1P | <i>PPPoE over IEEE 802.1Q</i>              |
| IEEE Standard 802.1Q | <i>Virtual Bridged Local Area Networks</i> |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title             |
|----------|-------------------|
| RFC 2516 | PPP over Ethernet |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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 | <p>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.</p> <p>In Cisco IOS XE Release 2.4, this feature was introduced.</p> <p>The following command was introduced: <b>control-packets vlan cos</b>.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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

© 2006–2009 Cisco Systems, Inc. All rights reserved.





# PPPoE Smart Server Selection

---

**First Published: April 18, 2008**

**Last Updated: June 19, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE Smart Server Selection”](#) section on [page 10](#).

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

## Contents

- [Information About PPPoE Smart Server Selection, page 2](#)
- [How to Configure PPPoE Smart Server Selection, page 2](#)
- [Configuration Examples for PPPoE Smart Server Selection, page 7](#)
- [Additional References, page 8](#)
- [Feature Information for PPPoE Smart Server Selection, page 10](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

**REVIEW DRAFT – CISCO CONFIDENTIAL**

# Information About PPPoE Smart Server Selection

To enable the PPPoE Smart Server Selection feature, you should understand the following concept:

- [Benefits of PPPoE Smart Server Selection, page 2](#)

## 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

This section contains the following procedures:

- [Configuring BBA Group PADO Delay](#) (optional)
- [Configuring PPPoE Service PADO Delay](#) (optional)
- [Configuring PPPoE Service PADO Delay](#) (optional)

## Configuring BBA Group PADO Delay

Perform this task to allow all calls coming into a defined BBA group on a 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 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*

**REVIEW DRAFT – CISCO CONFIDENTIAL**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                        | <b>Purpose</b>                                                                                                                                                                                                                                                                              |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                               | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                     |
| <b>Step 2</b> | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                          | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <p><b>bba-group pppoe</b> {group-name   global}</p> <p><b>Example:</b><br/>Router(config)# bba-group pppoe server-selection</p> | <p>Defines a PPP over Ethernet (PPPoE) profile, and enters BBA group configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>global</b> keyword creates a profile, which serves as the default profile for any PPPoE port that is not assigned a specific profile.</li> </ul> |
| <b>Step 4</b> | <p><b>pado delay</b> milliseconds</p> <p><b>Example:</b><br/>Router(config-bba-group)# pado delay 45</p>                        | <p>Sets the time by which a PADO response is delayed for a BBA group.</p> <p><b>Note</b> Setting a value of 0 means no transmission delay. Setting a value of 9999 means setting an infinite time (PADO is never sent).</p>                                                                 |

**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. If 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.) The preference for matching the string is described in the [DETAILED STEPS](#) table.

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.



**REVIEW DRAFT – CISCO CONFIDENTIAL**
**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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>bba-group pppoe</b> { <i>group-name</i>   <b>global</b> }                                                                                                                                                                              | Defines a PPPoE profile, and enters BBA group configuration mode. <ul style="list-style-type: none"> <li>• The <b>global</b> keyword creates a profile that serves as the default profile for any PPPoE port.</li> </ul>                                                                                                                                                                                   |
| Step 4 | <b>pppoe server circuit-id delay</b> <i>milliseconds</i> <b>string</b> [ <b>contains</b> ] <i>circuit-id-string</i><br><br><b>Example:</b><br>Router(config-bba-group)# pppoe server circuit-id delay 45 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. <ul style="list-style-type: none"> <li>• The <b>contains</b> keyword can find a partial match for this delay statement.</li> <li>• The value for the <i>circuit-id-string</i> argument can contain spaces when enclosed with double quotation marks (for example, "circuit ATM1/0/0 VC 0/100").</li> </ul> |
| Step 5 | <b>pppoe server remote-id delay</b> <i>milliseconds</i> <b>string</b> [ <b>contains</b> ] <i>remote-id-string</i><br><br><b>Example:</b><br>Router(config-bba-group)# pppoe server remote-id delay 30 string XTH-TEST                     | (Optional) Specifies the delay to be applied based on the PPPoE tag remote ID from the client. <ul style="list-style-type: none"> <li>• The <b>contains</b> keyword can find a partial match for this delay statement.</li> <li>• The value for the <i>remote-id-string</i> argument can contain spaces when enclosed with double quotation marks (for example, "subscr mac 1111.2222.3333").</li> </ul>   |

**REVIEW DRAFT – CISCO CONFIDENTIAL**

|               | <b>Command or Action</b>                                                                                                                     | <b>Purpose</b>                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b> | <p><b>pado delay</b> <i>circuit-id</i> <i>milliseconds</i></p> <p><b>Example:</b><br/>Router(config-bba-group)# pado delay circuit-id 35</p> | <p>(Optional) Finds a match based on the PPPoE group circuit ID delay if configured.</p> <ul style="list-style-type: none"> <li>If a circuit ID cannot be matched partially, a delay is applied based on any circuit ID that is present.</li> </ul> |
| <b>Step 7</b> | <p><b>pado delay remote-id</b> <i>milliseconds</i></p> <p><b>Example:</b><br/>Router(config-bba-group)# pado delay remote-id 30</p>          | <p>(Optional) Finds a match based on the PPPoE group remote ID delay if configured.</p>                                                                                                                                                             |
| <b>Step 8</b> | <p><b>pado delay</b> <i>milliseconds</i></p> <p><b>Example:</b><br/>Router(config-bba-group)# pado delay 45</p>                              | <p>(Optional) Uses the group PADO delay configuration.</p> <ul style="list-style-type: none"> <li>The PADO delay value is sought if the PADO delay is not found after several attempts.</li> </ul>                                                  |
| <b>Step 9</b> | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-bba-group)# end</p>                                                                   | <p>Ends the configuration session and returns to privileged EXEC mode.</p>                                                                                                                                                                          |

**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**

- enable**
- configure terminal**
- policy-map type service** *polycymap-name*
- exit**
- bba-group** [**global** | *profile-name*]
- virtual-template** *interface-number*
- service profile** *polycymap-name* **refresh** *minutes*
- service name match**
- end**

**REVIEW DRAFT – CISCO CONFIDENTIAL**

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                                                                  | <b>Purpose</b>                                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p><b>enable</b></p> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                         | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.5</li> </ul>                                                                                                                                                             |
| <b>Step 2</b> | <p><b>configure terminal</b></p> <p><b>Example:</b><br/>Router# configure terminal</p>                                                                                    | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                               |
| <b>Step 3</b> | <p><b>policy-map type service <i>policymap-name</i></b></p> <p><b>Example:</b><br/>Router(config)# policy-map type service serv3</p>                                      | <p>Places the router in service policy map configuration mode, and defines the name of service policy map.</p>                                                                                                                                                                         |
| <b>Step 4</b> | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                                        | <p>Exits configuration mode and returns to EXEC command mode.</p>                                                                                                                                                                                                                      |
| <b>Step 5</b> | <p><b>bba-group pppoe [<b>global</b>   <i>profile-name</i>]</b></p> <p><b>Example:</b><br/>Router(config-bba-group)# bba-group pppoe global</p>                           | <p>Defines a PPPoE profile, and enters BBA group configuration mode.</p> <ul style="list-style-type: none"> <li>• The <b>global</b> keyword creates a profile that serves as the default profile for any PPPoE port.</li> </ul>                                                        |
| <b>Step 6</b> | <p><b>virtual-template <i>interface-number</i></b></p> <p><b>Example:</b><br/>(config-bba-group)# virtual-template 20</p>                                                 | <p>Specifies the virtual template interface number for the BBA group, and places the router in configuration BBA group mode.</p>                                                                                                                                                       |
| <b>Step 7</b> | <p><b>service profile <i>subscriber-profile-name</i> refresh <i>minutes</i></b></p> <p><b>Example:</b><br/>Router(config-bba-group)# service profile serv3 refresh 30</p> | <p>Specifies the subscriber profile to be associated with the BBA group, and the refresh interval minutes for the service profile.</p>                                                                                                                                                 |
| <b>Step 8</b> | <p><b>service name match</b></p> <p><b>Example:</b><br/>Router(config-bba-group)# service name match</p>                                                                  | <p>Matches the requested tag for the PPPoE global group.</p> <p><b>Note</b> The <b>service name match</b> 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.</p> |
| <b>Step 9</b> | <p><b>end</b></p> <p><b>Example:</b><br/>(config-bba-group)# end</p>                                                                                                      | <p>Ends the configuration session and returns to privileged EXEC mode.</p>                                                                                                                                                                                                             |

**REVIEW DRAFT – CISCO CONFIDENTIAL**

## 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

This section provides the following configuration examples:

- [Configuring BBA Group PADO Delay: Example, page 7](#)
- [Configuring PADO Delay: Example, page 7](#)
- [Configuring PPPoE Service PADO Delay, page 5](#)
- [Verifying the PPPoE Service Match and PADO Delay: Example, page 8](#)

## Configuring BBA Group PADO Delay: Example

The following example shows how to configure a BBA group for PADO delay:

```
Router(config)# bba-group pppoe server-selection
Router(config-bba-group)# pado delay 45
```

## 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:

```
Router(config-bba-group)# pppoe server circuit-id delay 45 string "subscr mac
1111.2222.3333"
Router(config-bba-group)# pado delay circuit-id 35
Router(config-bba-group)# pado delay remote-id 30
```

The following example shows how to configure PADO delay based on the remote ID or circuit ID:

```
Router(config-bba-group)# pppoe server remote-id delay 20 string contains TEST
Router(config-bba-group)# pppoe server remote-id delay 10 string XTH
Router(config-bba-group)# pppoe server remote-id delay 30 string contains XTH-TEST
```

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 20. In this case, the first match succeeds and the configuration never reaches a delay of 30. 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:

```
Router(config)# policy-map type service XTH-services
Router(config-service-policymap)# pppoe service ILoBr delay 1000
Router(config-service-policymap)# pppoe service xth-service1 delay 500
Router(config-service-policymap)# pppoe service service-nodelay
Router(config-service-policymap)# exit
```

**REVIEW DRAFT—CISCO CONFIDENTIAL**

```
Router(config)# bba-group pppoe server-selection
Router(config-bba-group)# service svc-group
Router(config-bba-group)# service profile XTH-services
Router(config-bba-group)# service name match
Router(config-bba-group)# virtual-template 1
```

## 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.

```
Router# show pppoe derived group svc-group

Derived configuration from subscriber profile 'XTH-services':
Service names: servicename:pado-delay
ILoBr:1000, xth-service1:500, 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                               | <a href="#">Cisco IOS XE Broadband and DSL Configuration Guide</a>                                                                                                                                      |
| Additional information about commands used in this document | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a></li> <li><a href="#">Cisco IOS Master Command List, All Releases</a></li> </ul> |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**REVIEW DRAFT – CISCO CONFIDENTIAL****RFCs**

| <b>RFC</b> | <b>Title</b>                                               |
|------------|------------------------------------------------------------|
| RFC 2516   | <i>A Method for Transmitting PPP over Ethernet (PPPoE)</i> |

**Technical Assistance**

| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Link</b>                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

**REVIEW DRAFT – CISCO CONFIDENTIAL**

# Feature Information for PPPoE Smart Server Selection

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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. |

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0903R)

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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



# Monitoring PPPoE Sessions with SNMP

---

**First Published: May 2, 2005**

**Last Updated: February 20, 2010**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for Monitoring PPPoE Sessions with SNMP](#)” section on page 17.

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

## Contents

- [Prerequisites for Monitoring PPPoE Sessions with SNMP](#), page 2
- [Restrictions for Monitoring PPPoE Sessions with SNMP](#), page 2
- [Information About Monitoring PPPoE Sessions with SNMP](#), page 2
- [How to Configure Monitoring of PPPoE Sessions with SNMP](#), page 4
- [Configuration Examples for Monitoring PPPoE Sessions with SNMP](#), page 13



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**



- [Where to Go Next](#), page 14
- [Additional References](#), page 15
- [Feature Information for Monitoring PPPoE Sessions with SNMP](#), page 17

## 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 Sessions](#) 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

In order to perform monitoring of PPPoE sessions with SNMP, you should understand the following concepts:

- [Network Management Protocol](#), page 2
- [PPPoE Session Count MIB](#), page 2
- [Benefits of Monitoring PPPoE Sessions with SNMP](#), page 3

## 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.

Table 1 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 1** *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                                                                                                                        |
| 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

This section contains the following procedures:

- [Configuring the PPPoE Session-Count Threshold for the Router, page 4](#) (optional)
- [Configuring the PPPoE Session-Count Threshold for a PVC, page 5](#) (optional)
- [Configuring the PPPoE Session-Count Threshold for a VC Class, page 7](#) (optional)
- [Configuring the PPPoE Session-Count Threshold for an ATM PVC Range, page 8](#) (optional)
- [Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range, page 9](#) (optional)
- [Monitoring and Maintaining PPPoE Session Counts and SNMP Notifications, page 11](#) (optional)

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                     |

|        | Command or Action                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>snmp-server enable traps pppoe</pre> <p><b>Example:</b><br/>Router(config)# snmp-server enable traps pppoe</p>                                                  | (Optional) Enables PPPoE session count SNMP notifications. <ul style="list-style-type: none"> <li>This command enables SNMP traps that send notification messages when PPPoE sessions have been reached.</li> </ul>                                         |
| Step 4 | <pre>bba-group pppoe {group-name   global}</pre> <p><b>Example:</b><br/>Router(config)# bba-group pppoe global</p>                                                   | Configures a BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode.                                                                                                                                                      |
| Step 5 | <pre>sessions max limit session-number [threshold threshold-value]</pre> <p><b>Example:</b><br/>Router(config-bba-group)# sessions max limit 4000 threshold 3000</p> | 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. <p><b>Note</b> This command applies only to the global profile.</p> |
| Step 6 | <pre>virtual-template template-number</pre> <p><b>Example:</b><br/>Router(config-bba-group)# virtual-template 1</p>                                                  | Specifies the virtual template that will be used to clone the virtual access interfaces (VAI).                                                                                                                                                              |
| Step 7 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-bba-group)# end</p>                                                                                              | Exits BBA group configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                     |
| Step 8 | <pre>more system:running-config</pre> <p><b>Example:</b><br/>Router(#) more system:running-config</p>                                                                | 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

- enable
- configure terminal
- snmp-server enable traps pppoe
- interface atm slot/subslot/port[.subinterface] [multipoint | point-to-point]
- pvc [name] vpi/vci
- pppoe max-sessions number-of-sessions [threshold-sessions number-of-sessions]
- protocol pppoe
- end
- more system:running-config

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                               | Purpose                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                  | Enters global configuration mode.                                                                                                                                                                                             |
| Step 3 | <b>snmp-server enable traps pppoe</b><br><br><b>Example:</b><br>Router(config)# snmp-server enable traps pppoe                                                                                  | (Optional) Enables PPPoE session count SNMP notifications. <ul style="list-style-type: none"> <li>This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.</li> </ul> |
| Step 4 | <b>interface atm slot/subslot/port[.subinterface]</b><br><b>[multipoint   point-to-point]</b><br><br><b>Example:</b><br>Router(config)# interface atm 0/0/0.3<br>point-to-point                 | Configures the ATM interface and enters subinterface configuration mode.                                                                                                                                                      |
| Step 5 | <b>pvc [name] vpi/vci</b><br><br><b>Example:</b><br>Router(config-subif)# pvc 5/120                                                                                                             | Creates an ATM PVC and enters ATM VC configuration mode.                                                                                                                                                                      |
| Step 6 | <b>pppoe max-sessions number-of-sessions</b><br><b>[threshold-sessions number-of-sessions]</b><br><br><b>Example:</b><br>Router(config-if-atm-vc)# pppoe max-sessions 5<br>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 7 | <b>protocol pppoe</b><br><br><b>Example:</b><br>Router(config-if-atm-vc)# protocol pppoe                                                                                                        | Enables PPPoE sessions to be established on ATM PVCs.                                                                                                                                                                         |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-if-atm-vc)# end                                                                                                                              | (Optional) Exits ATM VC configuration mode and returns to sub interface mode.                                                                                                                                                 |
| Step 9 | <b>more system:running-config</b><br><br><b>Example:</b><br>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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                              | Enters global configuration mode.                                                                                                                                                                                                |
| Step 3 | <b>snmp-server enable traps pppoe</b><br><br><b>Example:</b><br>Router(config)# snmp-server enable traps pppoe                                                                                              | (Optional) Enables PPPoE session count SNMP notifications.<br><ul style="list-style-type: none"><li>• This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.</li></ul> |
| Step 4 | <b>vc-class atm</b> <i>name</i><br><br><b>Example:</b><br>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 | <b>pppoe max-sessions</b> <i>number-of-sessions</i> [ <b>threshold-sessions</b> <i>number-of-sessions</i> ]<br><br><b>Example:</b><br>Router(config-vc-class)# pppoe max-sessions 7<br>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 | <b>protocol pppoe</b> [ <b>group</b> <i>group-name</i>   <b>global</b> ]<br><br><b>Example:</b><br>Router(config-vc-class)# protocol pppoe group one                                                        | Enables PPPoE sessions to be established.                                                                                                                                                                                        |

|        | Command or Action                                                                                                   | Purpose                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-vc-class)# end</code>                                | (Optional) Exits VC class configuration mode and returns to privileged EXEC mode. |
| Step 8 | <code>more system:running-config</code><br><br><b>Example:</b><br><code>Router(#) more system:running-config</code> | Displays the running configuration and the PPPoE session-count thresholds.        |

## Configuring the PPPoE Session-Count Threshold for an ATM PVC Range

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 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                                     | Enters global configuration mode.                                                                                                                                                                                               |
| Step 3 | <code>snmp-server enable traps pppoe</code><br><br><b>Example:</b><br><code>Router(config)# snmp-server enable traps pppoe</code>                                                     | (Optional) Enables PPPoE session count SNMP notifications. <ul style="list-style-type: none"> <li>• This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.</li> </ul> |
| Step 4 | <code>interface atm slot/subslot/port[.subinterface] [multipoint   point-to-point]</code><br><br><b>Example:</b><br><code>Router(config)# interface atm 0/0/0.3 point-to-point</code> | Configures the ATM interface and enters the subinterface configuration mode.                                                                                                                                                    |

|        | Command or Action                                                                                                                                                                                                    | Purpose                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>range</b> [ <i>range-name</i> ] <b>pvc</b> <i>start-vpi/start-vci</i><br><i>end-vpi/end-vci</i><br><br><b>Example:</b><br>Router(config-subif)# range pvc 3/100 3/105                                             | Defines a range of ATM PVCs and enters ATM PVC range configuration mode.                                                                                                                          |
| Step 6 | <b>pppoe max-sessions</b> <i>number-of-sessions</i><br>[ <b>threshold-sessions</b> <i>number-of-sessions</i> ]<br><br><b>Example:</b><br>Router(config-if-atm-range)# pppoe max-sessions<br>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 | <b>protocol pppoe</b> [ <b>group</b> <i>group-name</i>   <b>global</b> ]<br><br><b>Example:</b><br>Router(config-if-atm-range)# protocol pppoe<br>group two                                                          | Enables PPPoE sessions to be established.                                                                                                                                                         |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-if-atm-range)# end                                                                                                                                                | (Optional) Exits ATM PVC range configuration mode and returns to privileged EXEC mode.                                                                                                            |
| Step 9 | <b>more system:running-config</b><br><br><b>Example:</b><br>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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                              |
| Step 3 | <b>snmp-server enable traps pppoe</b><br><br><b>Example:</b><br>Router(config)# snmp-server enable traps pppoe                                                                                       | (Optional) Enables PPPoE session count SNMP notifications.<br><ul style="list-style-type: none"><li>This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.</li></ul> |
| Step 4 | <b>interface atm slot/subslot/port[.subinterface]</b><br><b>[multipoint   point-to-point]</b><br><br><b>Example:</b><br>Router(config)# interface atm 6/0.110<br>multipoint                          | Configures the ATM interface and enters subinterface configuration mode.                                                                                                                                                       |
| Step 5 | <b>range [range-name] pvc start-vpi/start-vci</b><br><b>end-vpi/end-vci</b><br><br><b>Example:</b><br>Router(config-subif)# range range1 pvc 3/100<br>4/199                                          | Defines a range of ATM PVCs and enters ATM PVC Range configuration mode.                                                                                                                                                       |
| Step 6 | <b>pvc-in-range [pvc-name] [vpi/vci]</b><br><br><b>Example:</b><br>Router(config-if-atm-range)# pvc-in-range pvc1<br>3/104                                                                           | Configures an individual PVC within a PVC range and enters ATM PVC-in-range configuration mode.                                                                                                                                |
| Step 7 | <b>pppoe max-sessions number-of-sessions</b><br><b>[threshold-sessions number-of-sessions]</b><br><br><b>Example:</b><br>Router(cfg-if-atm-range-pvc)# pppoe<br>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 | <b>end</b><br><br><b>Example:</b><br>Router(cfg-if-atm-range-pvc)# end                                                                                                                               | (Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.                                                                                                                                      |
| Step 9 | <b>more system:running-config</b><br><br><b>Example:</b><br>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.

```
Router> enable
```

### Step 2

#### **debug snmp packets**

Use this command to display information about every SNMP packet sent or received by the router:

```
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.

```
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:

```
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:

```
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:

```
Router# show pppoe session

3 sessions in LOCALLY_TERMINATED (PTA) State
3 sessions total

Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VC: 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

This section provides the following configuration examples:

- [Configuring PPPoE Session-Count SNMP Traps: Example, page 13](#)
- [PPPoE Session-Count Threshold for the Router: Example, page 13](#)
- [PPPoE Session-Count Threshold for a PVC: Example, page 13](#)
- [PPPoE Session-Count Threshold for a VC Class: Example, page 14](#)
- [PPPoE Session-Count Threshold for a PVC Range: Example, page 14](#)
- [PPPoE Session-Count Threshold for an Individual PVC Within a PVC Range: Example, page 14](#)

## Configuring PPPoE Session-Count SNMP Traps: Example

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
```

## PPPoE Session-Count Threshold for the Router: Example

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 pppoel
 sessions max limit 4000 threshold 3000
 virtual-template 1
 pppoe limit max-sessions 4000 threshold-sessions 3000
```

## PPPoE Session-Count Threshold for a PVC: Example

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
```

## PPPoE Session-Count Threshold for a VC Class: Example

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
```

## PPPoE Session-Count Threshold for a PVC Range: Example

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                                                                                                                               | <a href="#">Understanding Broadband Access Aggregation</a>                                    |
| Tasks for preparing for broadband access aggregation                                                                                                                | <a href="#">Preparing for Broadband Access Aggregation</a>                                    |
| Configuring PPPoE sessions                                                                                                                                          | <a href="#">Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions</a> |
| Establishing PPPoE session limits for sessions on a specific PVC or VLAN configured on an L2TP access concentrator                                                  | <a href="#">Establishing PPPoE Session Limits per NAS Port</a>                                |
| Using service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup                                                         | <a href="#">Offering PPPoE Clients a Selection of Services During Call Setup</a>              |
| 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 | <a href="#">Enabling PPPoE Relay Discovery and Service Selection Functionality</a>            |
| Configuring the transfer upstream of the PPPoX session speed value                                                                                                  | <a href="#">Configuring Upstream Connection Speed Transfer</a>                                |
| Identifying a physical subscriber line for RADIUS communication with a RADIUS server                                                                                | <a href="#">Identifying the Physical Subscriber Line for RADIUS Access and Accounting</a>     |
| Configuring a Cisco Subscriber Service Switch                                                                                                                       | <a href="#">Configuring Cisco Subscriber Service Switch Policies</a>                          |

### 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:<br><a href="http://tools.cisco.com/ITDIT/MIBS/servlet/index">http://tools.cisco.com/ITDIT/MIBS/servlet/index</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Monitoring PPPoE Sessions with SNMP

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 2** Feature Information for Monitoring PPPoE Sessions with SNMP

| Feature Name                                                    | Releases                                                         | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PPPoE Session Count MIB,<br>SNMP Traps for PPPoE Session Limits | Cisco IOS XE<br>Release 2.5.0<br><br>Cisco IOS XE<br>Release 2.6 | <p>This feature was introduced on Cisco ASR 1000 Series Aggregation Routers.</p> <p>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.</p> <p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Information About Monitoring PPPoE Sessions with SNMP”</a> section on page 2</li> <li>• <a href="#">“How to Configure Monitoring of PPPoE Sessions with SNMP”</a> section on page 4</li> </ul> <p>The following commands were introduced or modified:</p> <p><b>snmp-server enable traps pppoe</b></p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)



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.

© 2005–2010 Cisco Systems, Inc. All rights reserved.



# PPPoE on ATM

---

**First Published: March 27, 2000**  
**Last Updated: November 25, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE on ATM” section on page 15](#)

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

## Contents

This document includes the following sections:

- [Prerequisites for PPPoE on ATM, page 2](#)
- [Restrictions for PPPoE on ATM, page 2](#)
- [Information About PPPoE on ATM, page 2](#)
- [How to Configure PPPoE on ATM, page 4](#)
- [Configuration Examples for PPPoE on ATM, page 12](#)
- [Additional References, page 13](#)
- [Feature Information for PPPoE on ATM, page 15](#)
- [Glossary, page 15](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## 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

The following restrictions apply when PPPoE on ATM is used:

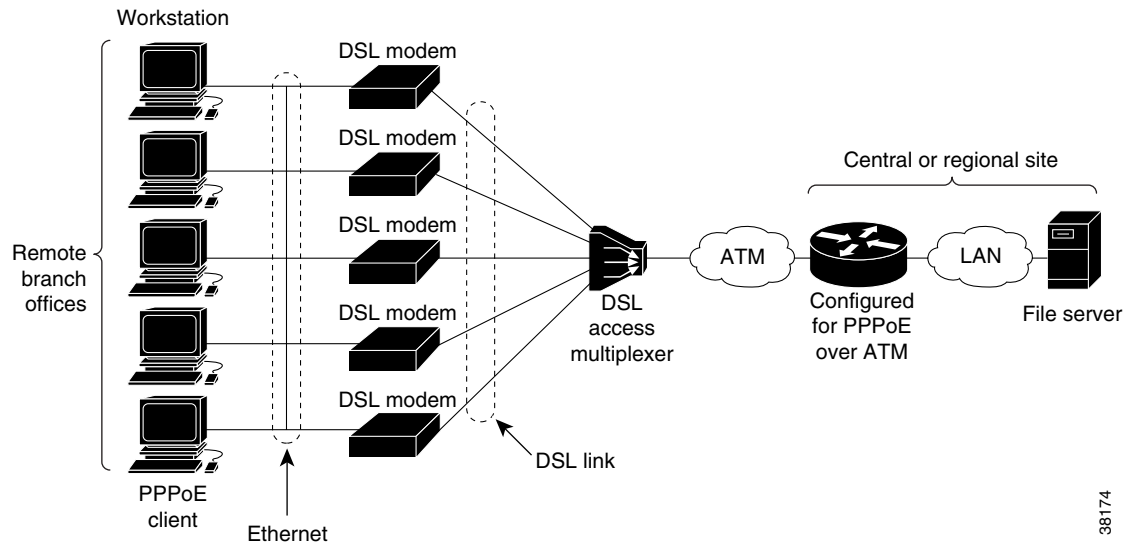
- PPPoE is not supported on Frame Relay.
- PPPoE over ATM AAL5Mux is not supported on ASR series 1000 routers. For more information, refer to the PPPoEoA over ATM AAL5Mux feature: [http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba\\_pppoeoa\\_aal5mux.html](http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba_pppoeoa_aal5mux.html)
- 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.

[Figure 1](#) shows a sample network topology using PPPoE on ATM.

**Figure 1** PPPoE on ATM Sample Network Topology



## PPPoE Stage Protocols

PPPoE has two distinct stage protocols. The stage protocols are listed and summarized in [Table 1](#).

**Table 1** 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 <i>must</i> 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

See the following sections for configuration tasks for the PPPoE on ATM feature. Each task in the list indicates if the task is optional or required.

- [Enabling PPP over ATM](#) (Required)
- [Creating and Configuring a Virtual Template](#) (Optional)
- [Specifying an ATM Subinterface](#) (Optional)
- [Creating an ATM PVC](#) (Required)
- [Enabling PPPoE on an ATM PVC](#) (Required)

## 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:

### 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]* [**multipoint** | **point-to-point**]
9. **ip address** *ip-address mask* [**secondary**]
10. **range** [*range-name*] **pvc** *start-vp/start-vci end-vp/end-vci*
11. **dbcs enable** [**aggregated** | **maximum**]
12. **protocol pppoe group** {*group-name* | **global**}  
or  
**encapsulation aal5snap**
13. **create-on-demand**
14. **end**



**Note**

You can use the **virtual-template**, **sessions per-vc**, and **sessions per-mac** commands in any order.

**DETAILED STEPS**

|               | <b>Command</b>                                                                                                                                                        | <b>Purpose</b>                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                              |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                |
| <b>Step 3</b> | <b>bba-group pppoe</b> { <i>group-name</i>   <b>global</b> }<br><br><b>Example:</b><br>Router(config)# bba-group pppoe pppoe-group                                    | Defines a PPPoE profile, and enters BBA group configuration mode.<br><ul style="list-style-type: none"><li>• The <b>global</b> keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.</li></ul>                                |
| <b>Step 4</b> | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config-bba-group)# virtual-template 1                                                 | Specifies which virtual template will be used to clone virtual access interfaces.                                                                                                                                                                                                                |
| <b>Step 5</b> | <b>sessions per-vc limit</b> <i>per-vc-limit</i> [ <b>threshold</b> <i>threshold-value</i> ]<br><br><b>Example:</b><br>Router(config-bba-group)# sessions max limit 1 | 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 Simple Network Management Protocol (SNMP) trap will be generated.<br><br><b>Note</b> This command applies only to the global profile. |

|         | Command                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre>sessions per-mac limit per-mac-limit</pre> <p><b>Example:</b><br/>Router(config-bba-group)# sessions per-mac limit 4000</p>                                                                                                                  | Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.                                                                                                                                                                                                                              |
| Step 7  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-bba-group)# exit</p>                                                                                                                                                                         | Exits BBA group configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                         |
| Step 8  | <pre>interface atm slot/subslot/port[.subinterface] [point-to-point   multipoint]</pre> <p><b>Example:</b><br/>Router(config)# interface atm 1/0.1 multipoint</p>                                                                                 | Specifies the ATM interface and enters subinterface configuration mode.                                                                                                                                                                                                                                              |
| Step 9  | <pre>ip address ip-address mask [secondary]</pre> <p><b>Example:</b><br/>Router(config-subif)# ip address 192.0.10.2 255.255.255.0 secondary</p>                                                                                                  | Sets a primary or secondary IP address for an interface.                                                                                                                                                                                                                                                             |
| Step 10 | <pre>range [range-name] pvc start-vpi/start-vci end-vpi/end-vci</pre> <p><b>Example:</b><br/>Router(config-if)# range pvc 101/304 200/400</p>                                                                                                     | Defines a range of ATM permanent virtual circuits (PVCs) and enters ATM range configuration mode.                                                                                                                                                                                                                    |
| Step 11 | <pre>dbns enable [aggregated   maximum]</pre> <p><b>Example:</b><br/>Router(config-if-atm-range)# dbns enable</p>                                                                                                                                 | Applies the Dynamic Subscriber Bandwidth Selection (DBS) QoS parameters.                                                                                                                                                                                                                                             |
| Step 12 | <pre>protocol pppoe group {group-name   global} or encapsulation aal5snap</pre> <p><b>Example:</b><br/>Router(config-if-atm-range-pvc)# protocol pppoe group two</p> <p>or</p> <pre>Router(config-if-atm-range-pvc)# encapsulation aal5snap</pre> | <p>Enables PPPoE sessions to be established on a PVC within a range.</p> <p>or</p> <p>Configures PPPoE autosense.</p> <ul style="list-style-type: none"> <li>If a PPPoE profile is not assigned to the PVC by using the <b>group</b> <i>group-name</i> option, the PVC will use the global PPPoE profile.</li> </ul> |

|         | Command                                                                                         | Purpose                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Step 13 | <b>create on-demand</b><br><br><b>Example:</b><br>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 | <b>end</b><br><br><b>Example:</b><br>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

Prior to configuring the ATM PVC for PPPoE on ATM, you typically create and configure a virtual template. To create and configure a virtual template, use the following commands:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template *number***
4. **encapsulation ppp**
5. **ip unnumbered gigabitethernet *slot/subslot/port*[.*subinterface*]**
6. **end**

### DETAILED STEPS

|        | Command                                                                                                                | Purpose                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                         | Enters global configuration mode.                                                                                  |
| Step 1 | <b>interface virtual-template <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface virtual-template 2 | Creates a virtual template, and enters interface configuration mode.                                               |
| Step 2 | <b>encapsulation ppp</b><br><br><b>Example:</b><br>Router(config-if)# encapsulation ppp                                | Enables PPP encapsulation on the virtual template.                                                                 |



|        | Command                                                                     | Purpose                                                                                |
|--------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Step 3 | <code>ip unnumbered gigabitethernet slot/subslot/port[.subinterface]</code> | Optionally, enables IP without assigning a specific IP address on the LAN.             |
|        | <b>Example:</b><br>Router(config-if)# ip unnumbered gigabitethernet0/0/0    |                                                                                        |
| Step 4 | <code>end</code>                                                            | (Optional) Exits the interface configuration mode and returns to privileged EXEC mode. |
|        | <b>Example:</b><br>Router(config-if)# end                                   |                                                                                        |

Other optional configuration commands can be added to the virtual template configuration. 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 spawn from a single virtual template; hence, multiple PVCs can use a single virtual template.

Cisco IOS software supports up to 25 virtual template configurations. If greater numbers of tailored configurations are required, an authentication, authorization, and accounting (AAA) server may be employed.

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

Network addresses for the PPP-over-ATM connections are not configured on the main ATM interface or subinterface. Instead, these connections are configured on the appropriate virtual template or obtained via AAA.

The virtual templates support all standard PPP configuration commands; however, not all configurations are supported by the PPP-over-ATM virtual access interfaces. These restrictions are enforced at the time the virtual template configuration is applied (cloned) to the virtual access interface. These restrictions are described in the following paragraphs.

Only standard first-in, first-out (FIFO) queueing is supported when applied to PPP-over-ATM virtual access interfaces. Other types of queueing that are typically configured on the main interface are not (for example, fair queueing). If configured, these configuration lines are ignored when applied to a PPP-over-ATM interface.

Although Cisco Express Forwarding (CEF) switching is supported, fast switching, flow, and optimum switching are not; these configurations are ignored on the PPP-over-ATM virtual access interface. CEF 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.

Because an ATM PVC is configured for this feature, the following standard PPP features are not applicable and should not be configured:

- Asynchronous interfaces

- Dialup connections
- Callback on PPP

## 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                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                    |
| Step 3 | <b>interface atm slot/subslot/port[.subinterface] [multipoint   point-to-point]</b><br><br><b>Example:</b><br>Router# interface atm 6/0.110 multipoint | Configures the ATM interface and enters subinterface configuration mode. <ul style="list-style-type: none"> <li>• A <b>multipoint</b> subinterface is recommended for interface conservation. A <b>point-to-point</b> subinterface will greatly restrict the total number of PPPoE sessions you can have.</li> </ul> |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config-subif)# end                                                                                         | (Optional) Exits the subinterface configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                            |

## Creating an ATM PVC

After you create a virtual template and specify an ATM subinterface, you must create an ATM PVC. To create 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. **encapsulation aal5snap**
6. **end**

**DETAILED STEPS**

|               | <b>Command</b>                                                                                                                                                           | <b>Purpose</b>                                                                                                     |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                           | Enters global configuration mode.                                                                                  |
| <b>Step 3</b> | <b>interface atm slot/subslot/port[.subinterface]</b><br><b>[multipoint   point-to-point]</b><br><br><b>Example:</b><br>Router(config)# interface atm 6/0.110 multipoint | Configures the ATM interface and enters subinterface configuration mode.                                           |
| <b>Step 1</b> | <b>pvc [name] vpi/vci</b><br><br><b>Example:</b><br>Router(config-subif)# pvc 5/120                                                                                      | Creates an ATM PVC and enters ATM VC configuration mode.                                                           |
| <b>Step 2</b> | <b>encapsulation aal5snap</b><br><br><b>Example:</b><br>Router(config-if-atm-vc)# encapsulation aal5snap                                                                 | Specifies AAL5 SNAP for ATM encapsulation.                                                                         |
| <b>Step 3</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-if-atm-vc)# end                                                                                                       | (Optional) Exits the ATM VC configuration mode and returns to privileged EXEC mode.                                |

The peak rate value is typically identical to the average rate or some suitable multiple thereof.

The average rate value should be set to the line rate available at the remote site, because the remote line rate will typically have the lowest speed of the connection.

For example, if the remote site has a T1 link, set the line rate to 1.536 Mbps. Because the average rate calculation on the ATM PVC includes the cell headers, a line rate value plus 10 or 15 percent may result in better remote line utilization.

The burst size depends on the number of cells that can be buffered by receiving ATM switches and is coordinated with the ATM network connection provider. If this value is not specified, the default, which is the equivalent to one maximum length frame on the interface, is used.

Operations, Administration and Maintenance (OAM) F5 cell loopback is provided by the remote AXIS shelf so OAM may be enabled. However, PPPoE on ATM is not typically an end-to-end ATM connection, and therefore enabling OAM is not recommended.

Once you configure the router for PPPoE on ATM, the PPP subsystem starts and the router attempts to send a PPP configure 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. After a timeout (typically 45 seconds), the router again attempts to reach the remote router by sending configuration requests.

## 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                                                                                                                                                                                  | Purpose                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                           | Enters global configuration mode.                                                                                  |
| Step 3 | <b>interface atm</b> <i>slot/subslot/port[.subinterface]</i><br>[ <b>multipoint</b>   <b>point-to-point</b> ]<br><br><b>Example:</b><br>Router(config)# interface atm 0/0/0.3 multipoint | Configures the ATM interface and enters the subinterface configuration mode.                                       |
| Step 4 | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i><br><br><b>Example:</b><br>Router(config-subif)# pvc 5/120                                                                                      | Creates an ATM PVC and enters ATM VC configuration mode.                                                           |

|        |                                                                                                                                                                                             |                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>pppoe max-sessions number-of-sessions [threshold-sessions number-of-sessions]</pre> <p><b>Example:</b><br/>Router(config-if-atm-vc)# pppoe max-sessions 5<br/>threshold-sessions 3</p> | 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 | <pre>protocol pppoe</pre> <p><b>Example:</b><br/>Router(config-if-atm-vc)# protocol pppoe</p>                                                                                               | Enables PPPoE sessions to be established on ATM PVCs.                                                                                                                                             |
| Step 7 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if-atm-vc)# end</p>                                                                                                                     | (Optional) Exits the ATM VC configuration mode and returns to privileged EXEC mode.                                                                                                               |

## Configuration Examples for PPPoE on ATM

This section provides the following configuration example:

- [PPPoE on ATM : Example, page 12](#)

### 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 from 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                                  | <i>Cisco IOS Master Commands List, All Releases</i>                          |
| Broadband and DSL commands                          | <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i>      |
| Enabling PPP authentication on the virtual template | <i>Configuring Virtual Template Interfaces</i>                               |
| Configuring an AAA server                           | <i>Configuring per-User Configuration</i>                                    |
| Configuring Broadband and DSL                       | <i>Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide</i> |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                          |
|----------|----------------------------------------------------------------|
| RFC 1483 | <i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i> |
| RFC 2364 | <i>PPP over AAL5</i>                                           |
| RFC 2516 | <i>A Method for Transmitting PPP over Ethernet (PPPoE)</i>     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for PPPoE on ATM

Table 2 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 2 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 2** Feature Information for PPPoE on ATM

| Feature Name | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PPPoE on ATM | Cisco IOS XE Release 2.5 | <p>This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>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.</p> <p>The following commands were introduced or modified:<br/> <b>bba-group, protocol (VPDN), virtual-template.</b></p> |

## 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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



# PPPoE on Ethernet

---

**First Published: March 31, 2000**  
**Last Updated: November 25, 2009**

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.

## Finding Feature Information

For the latest feature information and caveats, see 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 for PPPoE on Ethernet”](#) section on page 8.

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

## Contents

- [Prerequisites for PPPoE on Ethernet, page 2](#)
- [Restrictions for PPPoE on Ethernet, page 2](#)
- [Information About PPPoE on Ethernet, page 2](#)
- [How to Enable and Configure PPPoE on Ethernet, page 2](#)
- [Configuration Examples for PPPoE on Ethernet, page 5](#)
- [Additional References, page 6](#)
- [Feature Information for PPPoE on Ethernet, page 8](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## 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

The following restrictions apply when the PPPoE on Ethernet feature is used:

- 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

The following section has information about PPPoE on Ethernet:

- [Benefits of Using PPPoE on Ethernet, page 2](#)

## 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

The following sections contain configuration tasks for the PPPoE on Ethernet feature.

- [Enabling PPPoE on Ethernet in a VPDN Group, page 3](#) (required)
- [Limiting PPPoE Sessions from a MAC Address, page 4](#) (optional)
- [Creating and Configuring a Virtual Template, page 4](#) (optional)
- [Specifying an Ethernet Interface, page 4](#) (optional)
- [Enabling PPPoE on an Ethernet Interface, page 5](#) (required)
- [Monitoring and Maintaining VPDN Groups, page 5](#) (optional)

## 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. **vpdn enable**
2. **vpdn group** *name*
3. **accept dialin**
4. **protocol pppoe**
5. **virtual-template** *template-number*

### DETAILED STEPS

|               | <b>Command</b>                                                    | <b>Purpose</b>                                                                    |
|---------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>vpdn enable</b>                                | Enables virtual private dial-up networking.                                       |
| <b>Step 2</b> | Router(config-if)# <b>vpdn group</b> <i>name</i>                  | Associates a VPDN group to a customer or VPDN profile.                            |
| <b>Step 3</b> | Router(config-if)# <b>accept dialin</b>                           | Creates an accept dial-in VPDN group.                                             |
| <b>Step 4</b> | Router(config-if)# <b>protocol pppoe</b>                          | Specifies the VPDN group to be used to establish PPPoE sessions.                  |
| <b>Step 5</b> | Router(config-if)# <b>virtual-template</b> <i>template-number</i> | 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)# <b>pppoe session-limit per-mac</b> <i>number</i> | Sets the limit of sessions to be sourced from a MAC address. |

# Creating and Configuring a Virtual Template

To create and configure a virtual template, use the following commands beginning in global configuration mode:

|               | Command                                                         | Purpose                                                              |
|---------------|-----------------------------------------------------------------|----------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface virtual-template</b> <i>number</i> | Creates a virtual template, and enters interface configuration mode. |
| <b>Step 2</b> | Router(config-if)# <b>ip unnumbered ethernet</b> <i>number</i>  | Enables IP without assigning a specific IP address on the LAN.       |
| <b>Step 3</b> | Router(config-if)# <b>mtu</b> <i>bytes</i>                      | Sets the maximum transmission unit (MTU) size for the interface.     |

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 Solutions 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.

# 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# <b>interface ethernet</b> <i>interface-number</i> | Specifies the Ethernet interface using the appropriate format of the <b>interface ethernet</b> command. |

## Enabling PPPoE on an Ethernet Interface

To enable PPPoE on Ethernet interfaces, use the following command in global configuration mode:

| Command                           | Purpose                                                              |
|-----------------------------------|----------------------------------------------------------------------|
| Router# <code>pppoe enable</code> | 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# <code>show vpdn</code>                | Displays information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN. |
| Router# <code>show vpdn session packet</code> | Displays PPPoE session statistics.                                                                            |
| Router# <code>show vpdn session all</code>    | Displays PPPoE session information for each session ID.                                                       |
| Router# <code>show vpdn tunnel</code>         | Displays PPPoE session count for the tunnel.                                                                  |

## Configuration Examples for PPPoE on Ethernet

This section provides the following configuration examples:

- [PPPoE on Ethernet: Example](#)
- [Enabling PPPoE on an Ethernet Interface: Example](#)

### 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                       | <a href="#">PPPoE over ATM</a>                                                                                                                                                                                                 |
| Configuring PPPoE on cable interfaces          | <ul style="list-style-type: none"> <li><a href="#">Point-to-Point Protocol over Ethernet Support on the Cisco CMTS</a></li> <li><a href="#">Configuring PPPoE Termination on a uBR7100 CMTS with L2TP Tunneling</a></li> </ul> |
| Configuring PPPoE on IEEE 802.1Q encapsulation | <a href="#">PPPoE Over IEEE 802.1Q VLANs</a>                                                                                                                                                                                   |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                          |
|----------|----------------------------------------------------------------|
| RFC 2516 | <i>A Method for Transmitting PPPoE</i>                         |
| RFC 4813 | <i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |



# Feature Information for PPPoE on Ethernet

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Note**

Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

**Table 1** 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.<br><br>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. |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2000–2009 Cisco Systems, Inc. All rights reserved.



# Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

---

**First Published: May 2, 2005**

**Last Updated: November 10, 2010**

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Providing Connectivity Using ATM Routed Bridge Encapsulation”](#) section on page 16.

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

## Contents

- [Prerequisites for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs, page 2](#)
- [Restrictions for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs, page 2](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- [Information About Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs, page 2](#)
- [How to Configure ATM Routed Bridge Encapsulation over PVCs, page 5](#)
- [Configuration Examples for Providing Connectivity Using ATM Routed Bridge Encapsulation, page 11](#)
- [Additional References, page 14](#)
- [Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation, page 16](#)

## 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

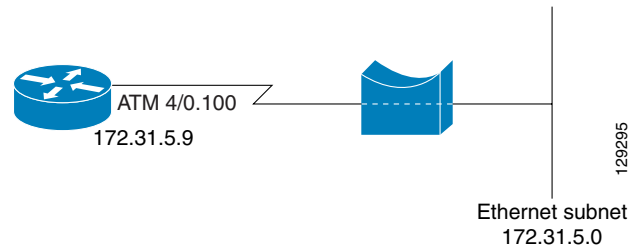
- [Overview on Bridged 1483 Encapsulated Traffic over ATM SVCs, page 2](#)
- [ATM RBE Subinterface Grouping by PVC Range, page 3](#)
- [ATM RBE Subinterface Grouping by PVC Range, page 3](#)
- [DHCP Option 82 Support for RBE, page 3](#)
- [DHCP Lease Limit per ATM RBE Unnumbered Interface, page 5](#)
- [Benefits of Providing Connectivity Using ATM Routed Bridge Encapsulation, page 5](#)

## 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.

Figure 1 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 1** 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:

$$\text{number of PVCs} = (\text{end-vpi} - \text{start-vpi} + 1) \times (\text{end-vci} - \text{start-vci} + 1)$$

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. Figure 2 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 2 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.

Figure 3 shows the format of the agent remote ID suboption.

**Figure 3 Format of the Agent Remote ID Suboption**

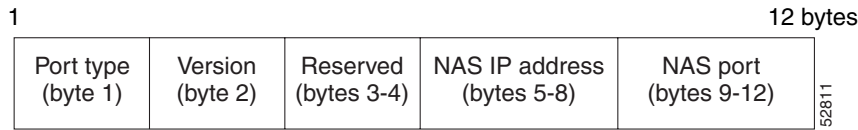


Table 1 describes the agent remote ID suboption fields displayed in Figure 3.

**Table 1 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 <b>rbe nasip</b> command can be used to specify which IP address will be used. (4 bytes) |
| NAS Port       | RBE-enabled virtual circuit on which the DHCP request has come in. See Figure 4 for the format of this field. (4 bytes)                     |

Figure 4 shows the format of the network access server (NAS) port field in the agent remote ID suboption.

**Figure 4 Format of the NAS Port Field**

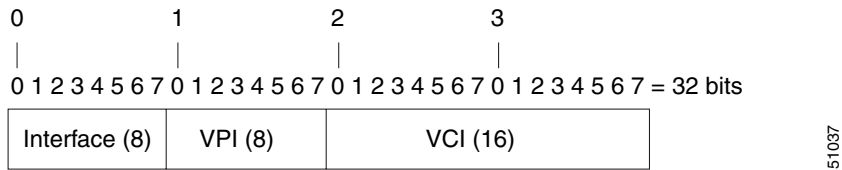
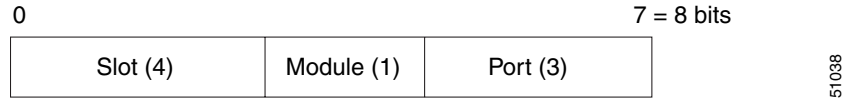


Figure 5 shows the format of the interface field. If there is no module, the value of the module bit is 0.

**Figure 5**      **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

This section contains the following procedures:

- [Configuring ATM Routed Bridge Encapsulation Using PVCs, page 6](#) (required)
- [Configuring DHCP Option 82 for RBE, page 8](#) (required)
- [Configuring the DHCP Lease Limit, page 10](#) (required)
- [Troubleshooting the DHCP Lease Limit, page 10](#) (optional)

## 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.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm slot/0.subinterface-number point-to-point**
4. **pvc vpi/vci**  
or  
**range [range-name] pvc start-vpi/start-vci end-vpi/end-vci**
5. **exit**
6. **ip address ip-address mask [secondary]**
7. **end**
8. **show arp**  
or  
**show ip cache verbose**

### DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                              | Enters global configuration mode.                                                                                  |
| Step 3 | <b>interface atm slot/0.subinterface-number point-to-point</b><br><br><b>Example:</b><br>Router(config)# interface atm 5/0.5 point-to-point | Specifies an ATM point-to-point subinterface and enters subinterface mode.                                         |

|        | Command or Action                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>pvc</b> <i>vpi/vci</i><br/>or</p> <p><b>range</b> [<i>range-name</i>] <b>pvc</b> <i>start-vpi/start-vci</i><br/><i>end-vpi/end-vci</i></p> <p><b>Example:</b><br/>Router(config-subif)# pvc 0/32<br/>or</p> <p><b>Example:</b><br/>Router(config-subif)# range range1 pvc 1/200<br/>1/299</p> | <p>Configures a PVC to carry the routed bridge traffic and enters ATM VC class configuration mode.</p> <p>Configures a range of PVCs to carry the routed bridge traffic and enters ATM PVC range configuration mode.</p> |
| Step 5 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-if-atm-vc)# exit</p>                                                                                                                                                                                                                        | Exits to subinterface configuration mode.                                                                                                                                                                                |
| Step 6 | <p><b>ip address</b> <i>ip-address mask</i> [<b>secondary</b>]</p> <p><b>Example:</b><br/>Router(config-subif)# ip address<br/>209.165.200.224 255.255.255.0</p>                                                                                                                                    | Provides an IP address on the same subnetwork as the remote network.                                                                                                                                                     |
| Step 7 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-subif)# end</p>                                                                                                                                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                           |
| Step 8 | <p><b>show arp</b><br/>or</p> <p><b>show ip cache verbose</b></p> <p><b>Example:</b><br/>Router# show arp<br/>or</p> <p><b>Example:</b><br/>Router# show ip cache verbose</p>                                                                                                                       | (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.

### Prerequisites for Configuring DHCP Option 82 for RBE

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

|        | Command                                                                                                                    | Purpose                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>ip dhcp relay information option</b></p> <p><b>Example:</b><br/>Router(config)# ip dhcp relay information option</p> | <p>Enables the DHCP option 82 support on relay agent.</p> <ul style="list-style-type: none"><li>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.</li></ul> |
| Step 4 | <p><b>rbe nasip source-interface</b></p> <p><b>Example:</b><br/>Router(config)# rbe nasip loopback0</p>                    | <p>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.</p>                                                                                                                                  |
| Step 5 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config)# end</p>                                                           | <p>Exits global configuration mode and enters privileged configuration mode.</p>                                                                                                                                                                                                 |

## 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                                                                                                                                   | Purpose                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                  |
| Step 3 | <b>ip dhcp limit lease per interface <i>lease-limit</i></b><br><br><b>Example:</b><br>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 | <b>end</b><br><br><b>Example:</b><br>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                                                                                                  | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug ip dhcp server packet</b><br><br><b>Example:</b><br>Router# debug ip dhcp server packet         | (Optional) Decodes DHCP receptions and transmissions.                                                            |
| Step 3 | <b>debug ip dhcp server events</b><br><br><b>Example:</b><br>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, page 11](#)
- [Example: Configuring ATM RBE on an Unnumbered Interface, page 11](#)
- [Example: Concurrent Bridging and ATM RBE, page 12](#)
- [Example: DHCP Option 82 for RBE Configuration, page 12](#)
- [Example: DHCP Lease Limit, page 13](#)

## 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 01010000B01018140580320. [Table 2](#) shows the value of each field within the agent remote ID suboption.

**Table 2 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 <ul style="list-style-type: none"> <li>• Interface (slot/module/port)</li> <li>• VPI</li> <li>• VCI</li> </ul> | <ul style="list-style-type: none"> <li>• 0x40 (The slot/module/port values are 01 00/0/000.)</li> <li>• 0x58 (hexadecimal value of 88)</li> <li>• 0x320 (hexadecimal value of 800)</li> </ul> |

## 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                              | <i>Cisco IOS Master Commands List, All Releases</i>                                                               |
| Broadband Access Aggregation and DSL commands   | <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i>                                           |
| Broadband access aggregation concepts           | <i>Understanding Broadband Access Aggregation</i>                                                                 |
| Preparing for broadband access aggregation task | <i>Preparing for Broadband Access Aggregation</i>                                                                 |
| DHCP commands                                   | <i>Cisco IOS IP Addressing Services Command Reference</i>                                                         |
| DHCP configuration tasks                        | “Configuring the Cisco IOS DHCP Server” module in the <i>Cisco IOS IP Addressing Services Configuration Guide</i> |

## 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |



# Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation

Table 3 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Table 3 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.

**Table 3** 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<br>12.2(33)SRE | <p>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.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Information About Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs” section on page 2</a></li> </ul> |

**Table 3** Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation (continued)

| Feature Name                                           | Releases             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Option 82 Support for Routed Bridge Encapsulation | 15.1(1)S<br>12.2(2)T | <p>This feature provides support for the DHCP relay agent information option when ATM RBE is used.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• “DHCP Option 82 Support for RBE” section on page 3</li> <li>• “Configuring DHCP Option 82 for RBE” section on page 8</li> </ul> <p>The following command was introduced:<br/><b>rbe nasip</b></p>                                                                                                                                                        |
| DHCP Lease Limit per ATM RBE Unnumbered Interface      | 12.3(2)T             | <p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• “DHCP Lease Limit per ATM RBE Unnumbered Interface” section on page 5</li> <li>• “Configuring the DHCP Lease Limit” section on page 10</li> </ul> <p>The following command was introduced:<br/><b>ip dhcp limit lease per interface</b></p> |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2005–2010 Cisco Systems, Inc. All rights reserved.





# PPP IP Unique Address and Prefix Detection

---

**First Published: November 24, 2010**  
**Last Updated: November 24, 2010**

The PPP IP Unique Address and Prefix Detection feature checks the uniqueness of IPv4 address and IPv6 prefix on the Broadband Remote Access Server (BRAS). PPP disconnects the session if it detects a duplicate IPv4 address and IPv6 prefix.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for PPP IP Unique Address and Prefix Detection”](#) section on page 5.

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

## Contents

- [“Information About PPP IP Unique Address and Prefix Detection”](#) section on page 1
- [“How to Configure PPP IP Unique Address and Prefix Detection”](#) section on page 2
- [“Configuration Examples for PPP IP Unique Address and Prefix Detection”](#) section on page 3
- [“Additional References”](#) section on page 4
- [“Feature Information for PPP IP Unique Address and Prefix Detection”](#) section on page 5

## 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.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                   | Enters global configuration mode.                                                                                  |
| Step 3 | <b>interface virtual-template</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface virtual-template 7 | Selects the Virtual Template interface and enters interface configuration mode.                                    |
| Step 4 | <b>ppp ipcp address required</b><br><br><b>Example:</b><br>Router(config-if)# ppp ipcp address required                          | PPP disconnects the peer if no IP address is negotiated.                                                           |
| Step 5 | <b>ppp ipcp address unique</b><br><br><b>Example:</b><br>Router(config-if)# ppp ipcp address unique                              | PPP disconnects the peer if the IP address is already in use.                                                      |

|         | Command or Action                                                                                                          | Purpose                                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <code>ppp ipv6cp address unique</code><br><br><b>Example:</b><br>Router(config-if)# <code>ppp ipv6cp address unique</code> | PPP disconnects the peer if the IPv6 prefix is already in use.                                                                                     |
| Step 7  | <code>ppp timeout ncp seconds</code><br><br><b>Example:</b><br>Router(config-if)# <code>ppp timeout ncp 30</code>          | PPP sets the maximum time in seconds to wait for the network layer to negotiate.                                                                   |
| Step 8  | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# <code>exit</code>                                           | Exits interface configuration mode and returns to global configuration mode.                                                                       |
| Step 9  | <code>ppp ncp override local</code><br><br><b>Example:</b><br>Router(config)# <code>ppp ncp override local</code>          | PPP overrides the local dual-stack configuration, checks the permitted Network Control Programs (NCP), and rejects user-initiated NCP negotiation. |
| Step 10 | <code>end</code><br><br><b>Example:</b><br>Router(config)# <code>end</code>                                                | Exits global configuration mode and returns to privileged EXEC mode.                                                                               |

## Configuration Examples for PPP IP Unique Address and Prefix Detection

This section provides the following configuration example:

- [Example: PPP Unique Address and Prefix Detection, page 3](#)

### Example: PPP Unique Address and Prefix Detection

To enable the PPP IP Unique Address and 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                                                          |
|-----------------------------------------------|-------------------------------------------------------------------------|
| Cisco IOS commands                            | <i>Cisco IOS Master Commands List, All Releases</i>                     |
| Broadband Access Aggregation and DSL commands | <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i> |

## 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## 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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# Feature Information for PPP IP Unique Address and Prefix Detection

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 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.

**Table 1** 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.<br><br>The following commands were introduced: <b>ppp ipv6cp address unique</b> , <b>ppp ncp override local</b> . |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.







## **High Availability**





# Broadband High Availability Stateful Switchover

---

**First Published: December 4, 2006**

**Last Updated: March 14, 2011**

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Broadband High Availability Stateful Switchover, page 19](#).

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

## Contents

- [Prerequisites for Broadband High Availability Stateful Switchover, page 2](#)
- [Restrictions for Broadband High Availability Stateful Switchover, page 2](#)
- [Information About Broadband High Availability Stateful Switchover, page 2](#)
- [How to Configure Broadband High Availability Stateful Switchover, page 4](#)
- [Configuration Examples for Broadband High Availability Stateful Switchover, page 12](#)
- [Additional References, page 16](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

- [Feature Information for Broadband High Availability Stateful Switchover, page 19](#)

## 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, page 2](#)
- [Benefits of Broadband High Availability Stateful Switchover, page 4](#)

## 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](#)” section on page 5.

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, page 3](#)
- [SSO L2TP, page 3](#)
- [SSO PPPoE, page 3](#)
- [SSO RA-MLPS VPN, page 3](#)

### 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

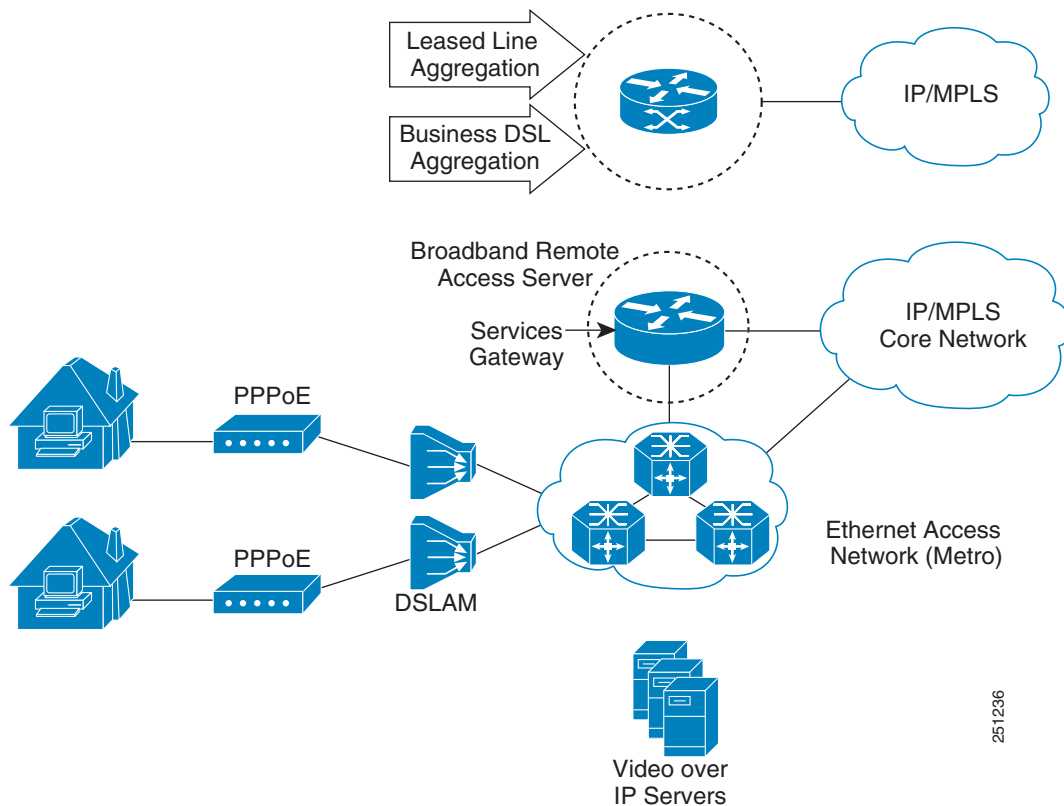
The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoEoVLAN, and PPPoEoQinQ.

### 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.

[Figure 1](#) shows a typical broadband aggregation HA deployment with SSO functionality.

**Figure 1** *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, page 5](#)
- [Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA Stateful Switchover, page 6](#)

# 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |



|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>subscriber redundancy</b> {<b>bulk limit</b> {<b>cpu percent</b> <b>delay seconds</b> [<b>allow sessions</b>]   <b>time seconds</b>}   <b>dynamic limit</b> <b>cpu percent</b> <b>delay seconds</b> [<b>allow sessions</b>]   <b>delay seconds</b>   <b>rate sessions seconds</b>}</p> <p><b>Example:</b><br/>Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30</p> | <p>(Optional) Configures subscriber redundancy policy.</p> <ul style="list-style-type: none"> <li>• <b>bulk</b>—Configures bulk synchronization redundancy policy.</li> <li>• <b>limit</b>—Specifies the limit for the synchronization.</li> <li>• <b>cpu percent</b>—Specifies a CPU busy threshold value as a percentage. Range is from 0 to 100; default is 90.</li> <li>• <b>delay seconds</b>—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.</li> <li>• <b>allow sessions</b>—(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.</li> <li>• <b>dynamic</b>—Configures a dynamic synchronization redundancy policy.</li> <li>• <b>rate sessions seconds</b>—Specifies the number of sessions per time period for bulk and dynamic synchronization. <ul style="list-style-type: none"> <li>– <i>sessions</i>—Range is from 1 to 32000; default is 250.</li> <li>– <i>seconds</i>—Range in seconds is from 1 to 33550; default is 1.</li> </ul> </li> </ul> |
| Step 4 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                                                                                                                                                                                                                                                                | <p>Exits global configuration mode and returns to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## 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”](#) section on page 12.

### 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**

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

```
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

```
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

```
Router# show ccm sessions
```

```
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFF
```

```
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

```
Router# show ccm sessions
```

```
Global CCM state: CCM HA Standby - Collecting
Global ISSU state: Compatible, Clients Cap 0x9EFFF
```

```
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:

```
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:

```
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:

```
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.

```

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.

```

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:

```

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 encaps change notification so far
0 : VC activation notifications received from ATM
0 : VC encaps change notifications received from ATM
0 : Total queued sessions waiting for VC notification(Encaps 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:

```
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:

```
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.

```
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

This section provides the following configuration example:

- [Example: Configuring Broadband High Availability Stateful Switchover, page 12](#)

## 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 commands                                      | <a href="#">Cisco IOS Master Command List, All Releases</a>                                                                                 |
| Cisco IOS Broadband Access Aggregation and DSL commands | <a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a>                                                            |
| High Availability                                       | “High Availability Overview” chapter in the <a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a> |

| Related Topic                  | Document Title                                                                                                                                                                                                                                                                |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Performing an ISSU             | The following chapters in the <i>Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</i> : <ul style="list-style-type: none"> <li>“Cisco IOS XE Software Package Compatibility for ISSU”</li> <li>“In Service Software Upgrade (ISSU)”</li> </ul> |
| 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## 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                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>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.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for Broadband High Availability Stateful Switchover

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 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.

**Table 1** 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.<br><br>The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over ATM (PPPoA) sessions during RP switchover.<br><br>The following commands were introduced or modified:<br><b>subscriber redundancy, debug pppatm redundancy, debug pppoe redundancy, show pppoe redundancy, show pppatm statistics.</b>                                                                                                                                                                                                                                        |
| SSO—PPPoE    | Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 2.5 | In Cisco IOS XE Release 2.1, this feature was implemented on ASR 1000 Series Routers.<br><br>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.<br><br>The following commands were introduced or modified:<br><b>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.</b> |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2006–2011 Cisco Systems, Inc. All rights reserved





# Broadband High Availability In-Service Software Upgrade

---

**First Published: December 4, 2006**  
**Last Updated: March 29, 2011**

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Broadband High Availability In-Service Software Upgrade” section on page 18](#).

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

## Contents

- [Prerequisites for Broadband High Availability In-Service Software Upgrade, page 2](#)
- [Restrictions for Broadband High Availability In-Service Software Upgrade, page 2](#)
- [Information About Broadband High Availability In-Service Software Upgrade, page 2](#)
- [How to Configure Broadband High Availability In-Service Software Upgrade, page 5](#)
- [Configuration Examples for Broadband High Availability In-Service Software Upgrade, page 11](#)
- [Additional References, page 16](#)
- [Feature Information for Broadband High Availability In-Service Software Upgrade, page 18](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**



# 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, page 2](#)
- [Benefits of Broadband High Availability In-Service Software Upgrade, page 4](#)

## 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”](#) section on page 5.

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, page 3](#)
- [ISSU L2TP, page 3](#)
- [ISSU PPPoE, page 3](#)
- [ISSU RA-MLPS VPN, page 3](#)

### 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

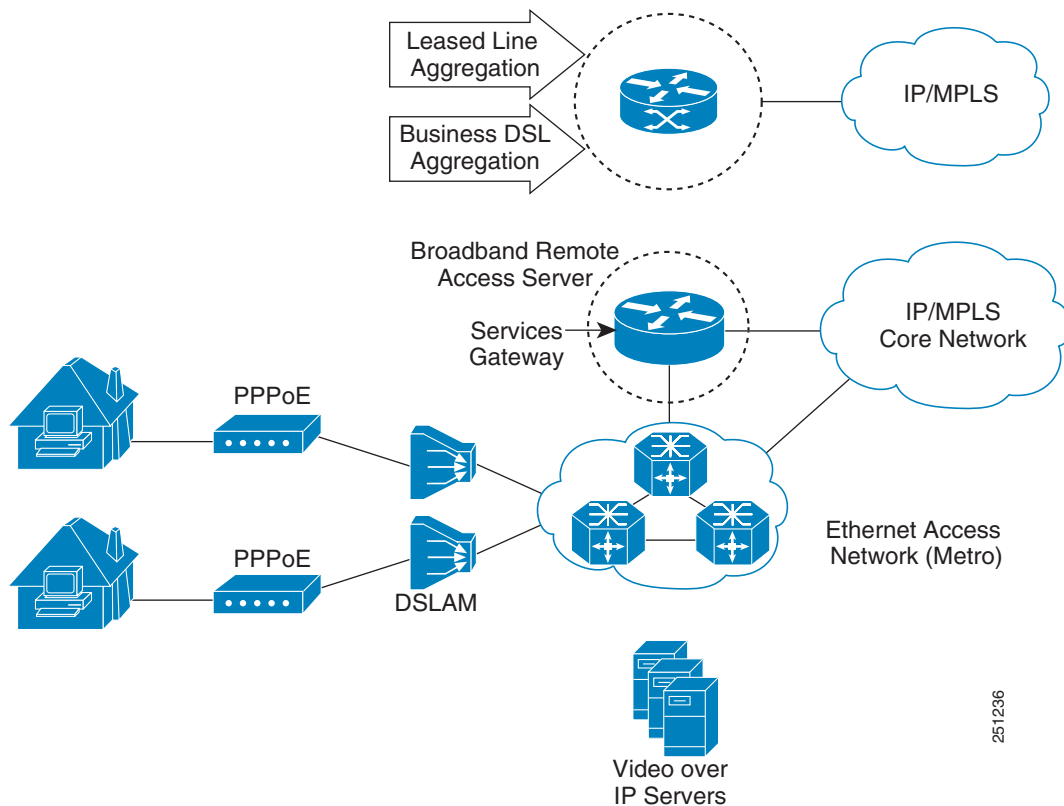
The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoE over VLAN, and PPPoE over QinQ sessions, during supported software upgrades, downgrades, and enhancements.

### 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.

[Figure 1](#) shows a typical broadband aggregation HA deployment with ISSU functionality.

**Figure 1** *Broadband Aggregation High Availability Deployment*



251236

## 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

This section contains the following procedures:

- [Configuring Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade, page 5](#) (required)
- [Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA ISSU, page 6](#) (optional)

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                       |

|        | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Step 3 | <pre>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}</pre> <p><b>Example:</b><br/>Router(config)# subscriber redundancy bulk<br/>limit cpu 75 delay 20 allow 30</p> | (Optional) Configures subscriber redundancy policy. |
| Step 4 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                                                                                                                                                                                            | 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](#)” section on page 11.

- [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.

```
Router# show ccm clients
```

```
CCM bundles sent since peer up:
 Sync Session Sent Queued for flow control
 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.

```
Router# show ccm sessions
```

```
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFF

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 0 - -
Dynamic CPU 00:00:10 - 0 0 90 0
Bulk CPU Lim 00:00:10 - 0 0 90 0
Bulk Time Li 00:00:01 - 0 0 - -
RF Notif Ext 00:00:01 - 8 0 - -
```

### 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.

```
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
2 3 Sync Client 0 0 0 0 0
3 3 Update 0 0 0 0 0
4 3 Session Down 0 0 0 0 0
5 3 Bulk Sync Begi 1 0 1 0 0
6 3 Bulk Sync Cont 2 0 2 0 0
7 3 Bulk Sync End 1 0 1 0 0
8 3 Rcv Bulk End 0 0 0 0 0
9 3 Dynamic Sync C 0 0 0 0 0
10 3 Going Active 0 0 0 0 0
11 3 Going Standby 0 0 0 0 0
12 3 Standby Presen 1 0 1 0 0
13 3 Standby Gone 0 0 0 0 0
15 3 CP Message 205 0 8 141 1000
16 3 Recr Session 0 0 0 0 0
17 3 Recr Update 0 0 0 0 0
18 3 Recr Sess Down 0 0 0 0 0
19 3 ISSU Session N 1 0 1 0 0
20 3 ISSU Peer Comm 0 0 0 0 0
21 3 Free Session 0 0 0 0 0
22 3 Sync Dyn Sessi 0 0 0 0 0
23 3 Recr Dyn Sessi 0 0 0 0 0
24 3 Session Ready 0 0 0 0 0
25 3 Pending Update 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.

```
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.

```
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.

```
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
PPPSbindResp 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.

```
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.

```
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.

```
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.

```
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

This section provides the following configuration examples:

- [Example: Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade, page 11](#)

### 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 vrfl
 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 commands                                          | <a href="#">Cisco IOS Master Commands List, All Releases</a>                                                                                                                                                                                                                           |
| Cisco IOS Broadband commands                                | <a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a>                                                                                                                                                                                                       |
| High Availability                                           | “High Availability Overview” chapter in the <a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a>                                                                                                                                            |
| Performing an ISSU                                          | The following chapters in the <a href="#">Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</a> : <ul style="list-style-type: none"> <li>“Cisco IOS XE Software Package Compatibility for ISSU”</li> <li>“In Service Software Upgrade (ISSU)”</li> </ul> |
| Broadband SSO                                               | <a href="#">Broadband High Availability Stateful Switchover</a>                                                                                                                                                                                                                        |
| Stateful switchover                                         | <a href="#">Stateful Switchover</a>                                                                                                                                                                                                                                                    |
| Cisco nonstop forwarding                                    | <a href="#">Cisco Nonstop Forwarding</a>                                                                                                                                                                                                                                               |
| Layer 2 Tunnel Protocol                                     | <a href="#">Layer 2 Tunnel Protocol Technology Brief</a>                                                                                                                                                                                                                               |
| Additional information about commands used in this document | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS Broadband Access Aggregation and DSL Command Reference</a></li> <li><a href="#">Cisco IOS Master Command List, All Releases</a></li> </ul>                                                                                |

## 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## 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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |



# Feature Information for Broadband High Availability In-Service Software Upgrade

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 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.

**Table 1** 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                            | <p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>This feature uses the ISSU support for PPPoA to ensure continuous operations of broadband access protocols during software upgrades.</p> <p>The following commands were introduced or modified:<br/> <b>debug pppatm redundancy, debug pppoe redundancy, show pppoe redundancy, show pppatm redundancy, show pppatm statistics, subscriber redundancy</b></p>                                                                                       |
| ISSU—PPPoE   | Cisco IOS XE Release 2.1<br>Cisco IOS XE Release 2.5 | <p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>This feature uses the ISSU—PPPoE support to ensure continuous operations of broadband access protocols during software upgrades, downgrades, and service enhancements.</p> <p>The following commands were introduced or modified:<br/> <b>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</b></p> |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2006–2011 Cisco Systems, Inc. All rights reserved