Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS XE Release 2

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

CONTENTS

Preparing for Broadband Access Aggregation

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

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 Table at the end of this document.

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

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

Virtual Access Interfaces

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

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

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

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

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

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

Configuration Enhancements for Broadband Scalability

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

Virtual Access Subinterfaces

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

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

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

Virtual Template Compatibility with Subinterfaces

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

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

Benefits of Broadband Scalability Features

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

How to Prepare for Broadband Access Aggregation

Configuring a Virtual Template Interface

Configure a virtual template 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**Interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**ip unnumbered loopback** *number* **Example:** `Router(config-if)# ip unnumbered loopback 0`	Enables IP without assigning a specific IP address on the LAN.
Step 5	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1492`	(Optional) Sets the maximum MTU size for the interface. **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.
Step 6	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 7	**ppp ipcp ip address required** **Example:** `Router(config-if)# ppp ipcp ip address required`	Prevents a PPP session from being set up without a valid address being negotiated. This command is required for legacy dialup and DSL networks.

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

Examples

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

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

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

Subinterfaces cannot be created using
Virtual-Template1
```

```
Interface commands:
traffic-shape rate 50000 8000 8000 1000
```

Configuration Examples for Preparing for Broadband Access Aggregation

Virtual Access Subinterfaces Configuration Examples

This section provides the following configuration examples:

Virtual Access Subinterface Configuration Example

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

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

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

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

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

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


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

Testing a Virtual Template for Compatibility with Subinterfaces Example

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

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

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Preparing for Broadband Access Aggregation

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

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

Table 1 Feature Information for Preparing for Broadband Aggregation

Feature Name	Software Releases	Feature Configuration Information
Virtual Sub-Interface--Configuration Enhancements for Broadband Scalability	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. This feature reduces the amount of memory that is used per terminated PPP session by creating virtual access subinterfaces. Depending on the configuration of the source virtual template, virtual access subinterface may be available. This feature also introduces a command to determine if a virtual template is compatible with virtual access subinterfaces.

Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

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

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 Table at the end of this document.

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

Prerequisites for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

- You must understand the concepts described in the Understanding Broadband Access Aggregation module.
- You must perform the tasks contained in the Preparing for Broadband Access Aggregation module.

Restrictions for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

If a PPPoE profile is assigned to a PPPoE port (Gigabit Ethernet interface or PVC), virtual circuit (VC) class, or ATM PVC range and the profile has not yet been defined, the port, VC class, or range will not have any PPPoE parameters configured and will not use parameters from the global group.

The subscriber features that are supported/ not supported on PPP sessions are listed in the table below:

Table 2 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 up to 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
Per Subscriber QPPB	Not supported
MLPPP on LNS, MLPoE on PTA, MLPoE LAC Switching	Supported. For more information refer to the Wide Area Configuration Guide.
VLAN range	Not supported

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

PPPoE Specification Definition

PPP over Ethernet (PPPoE) is a specification that defines how a host PC interacts with common broadband medium (for example, a digital subscriber line (DSL), wireless modem or cable modem) to achieve access to a high-speed data network. Relying on two widely accepted standards, Gigabit Ethernet and PPP, the PPPoE implementation allows users over the Gigabit Ethernet to share a common connection. The Gigabit Ethernet principles supporting multiple users in a LAN, combined with the principles of PPP, which apply to serial connections, support this connection.

The base protocol is defined in RFC 2516.

PPPoE Connection Throttling

Repeated requests to initiate PPPoE sessions can adversely affect the performance of a router and RADIUS server. The PPPoE Connection Throttling feature limits PPPoE connection requests to help prevent intentional denial-of-service attacks and unintentional PPP authentication loops. This feature implements session throttling on the PPPoE server to limit the number of PPPoE session requests that can be initiated from a MAC address or VC during a specified period of time.

PPPoE VLAN Session Throttling

This feature throttles the number of PPPoE over QinQ sessions over each subinterface. If the number of new incoming session requests on the subinterface, exceeds the configured incoming session setup rate, the new session requests will be rejected. You can enable this capability independently on each Gigabit Ethernet subinterface.

The number of incoming session requests will be calculated separately on a combination of each port and subinterface, independent of each other. For example, if there are 2 subinterfaces sharing the QinQ VLAN IDs, the session rate of each is calculated separately. You should assign the bba-group configuration on each subscriber subinterface, with an unambiguous VLAN or outer and inner VLAN IDs (in the case of QinQ).

Autosense for ATM PVCs

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

Note The PPPoA/PPPoE Autosense for ATM PVCs feature is supported on Subnetwork Access Protocol (SNAP)-encapsulated ATM PVCs only. It is not supported on multiplexer (MUX)-encapsulated PVCs.

- Benefits of Autosense for ATM PVCs, page 14

Benefits of Autosense for ATM PVCs

Autosense for ATM PVCs provides resource allocation on demand. For each PVC configured for PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoE session on that PVC. The autosense for ATM PVCs resources are allocated for PPPoE sessions only when a client initiates a session, thus reducing overhead on the NAS.

Note Autosense for ATM PVCs supports ATM PVCs only. Switched virtual circuits (SVCs) are not supported.

MAC Address for PPPoEoA

To prevent customers from experiencing unexpected behavior resulting from a system change, any change in the usage of MAC addresses will not happen unless it is explicitly configured.

Except for using a different MAC address, this feature does not change the way PPPoE works. This change is limited to ATM interfaces only--specifically, PPPoEoA--and will not be applied to other interfaces where PPPoE is operated on interfaces such as Gigabit Ethernet, Ethernet VLAN, and Data-over-Cable Service Interface Specifications (DOCSIS). Changing the PPPoE MAC address on those interfaces, which are broadcast in nature, requires placing the interface in promiscuous mode, thereby affecting the performance of the router because the router software has to receive all Gigabit Ethernet frames and then discard unneeded frames in the software driver.

This feature is disabled by default and applies to all PPPoE sessions on an ATM PVC interface configured in a BBA group.

When PPPoE and 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, page 15

Benefits of the Configurable MAC Address for PPPoE Feature

Because the Cisco IOS XE aggregation routers use the interface MAC address as the source MAC address for all broadband aggregation protocols on that interface, this feature solves problems that may occur when both RBE and PPPoE are deployed on the same ATM interface.

How to Provide Protocol Support for Broadband Access Aggregation of PPPoE Sessions

To provide protocol support for broadband access aggregation by assigning a profile, defining the profile is required. The profile definition is required as described in the Defining a PPPoE Profile, page 15, and an additional task makes an assignment of the profile to a protocol type.

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

Defining a PPPoE Profile

Perform this task to define a PPPoE profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*]
6. **sessions per-mac limit** *per-mac-limit*
7. **sessions per-vlan limit** *per-vlan-limit* **inner** *per-inner-vlan-limit*
8. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
9. **sessions** {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period*
10. **ac name** *name*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 8000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold at which an Simple Network Management Protocol (SNMP) trap will be generated. **Note** This command applies only to the global profile.
Step 6	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 2`	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.

	Command or Action	Purpose
Step 7	**sessions per-vlan limit** *per-vlan-limit* **inner** *per-inner-vlan-limit* **Example:** `Router(config-bba-group)# sessions per-vlan limit 200`	Sets the maximum number of PPPoE sessions permitted per VLAN in a PPPoE profile. • The **inner** keyword sets the number of sessions permitted per outer VLAN.
Step 8	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit 8`	Sets the maximum number of PPPoE sessions permitted on a VC in a PPPoE profile, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 9	**sessions** {**per-mac** | **per-vc** | **per-vlan**} **throttle** *session-requests session-request-period blocking-period* **Example:** `Router(config-bba-group)# sessions per-vc throttle 100 30 3008`	(Optional) Configures PPPoE connection throttling, which limits the number of PPPoE session requests that can be made from a VLAN, VC, or a MAC address within a specified period of time.
Step 10	**ac name** *name* **Example:** `Router(config-bba-group)# ac name ac1`	(Optional) Specifies the name of the access concentrator to be used in PPPoE active discovery offers (PADOs).
Step 11	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Exits BBA group configuration mode and returns to privileged EXEC mode.

Enabling PPPoE on an Interface

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *number*
4. **encapsulation dot1q second-dot1q** {**any** | *vlan-id*}
5. **pppoe enable** [**group** *group-name*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *number* **Example:** `Router(config)# interface gigabitethernet 0/0/0.0`	Specifies an Gigabit Ethernet interface and enters interface configuration mode.
Step 4	**encapsulation dot1q second-dot1q** {**any** | *vlan-id*} **Example:** `Router(config-subif)# encapsulation dot1q second-dot1q 1`	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
Step 5	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group one`	Enables PPPoE sessions on an Gigabit Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface by using the **group** *group-name* option, the interface will use the global PPPoE profile.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-subif)# end`	(Optional) Exits subinterface configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM PVC

Perform this task to assign a PPPoE profile to an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **pvc** *vpi* / *vci*
5. Do one of the following:
    - **protocol pppoe** [**group** *group-name*]
    -
    - **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. • 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.

	Command or Action	Purpose
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	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	•
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	
	Example:
	
	`Router(config-if-atm-vc)# protocol pppoe group one`
	
	Example:
	
	Example:
	
	`Router(config-if-atm-vc)# encapsulation aal5autoppp virtual-template 1 group one`
		Enables PPPoE sessions to be established on ATM PVCs.
		
		or
		
		Configures PPPoE autosense on the PVC.
		
		Note If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

Step 6	**end** **Example:** `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-vpi* / *start-vci end-vpi* / *end-vci*
5. **protocol pppoe** [**group** *group-name*]
6. **pvc-in-range** [*pvc-name*] [[*vpi* /]*vci*]
7. Do one of the following:
   - **protocol pppoe** [**group** *group-name*]
   -
   - or
   - **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-if)# range range-one pvc 100 4/199`	Defines a range of PVCs and enters ATM PVC range configuration mode.

	Command or Action	Purpose

Step 5	**protocol pppoe** [**group** *group-name*]
	
	Example:
	
	Example:
	`or`
	
	Example:
	
	encapsulation aal5autoppp virtual-template *number* [**group** *group-name*]
	
	Example:
	`Router(config-if-atm-range)# protocol pppoe group one`
	
	Example:
	
	Example:
	`or`
	
	Example:
	`Router(config-if-atm-range)# encapsulation aal5autoppp 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** *group-name* option, the PVCs in the range will use the global PPPoE profile.

Step 6	**pvc-in-range** [*pvc-name*] [[*vpi* /]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Defines an individual PVC within a PVC range and enables ATM PVC-in-range configuration mode.

	Command or Action	Purpose

Step 7	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	•
	• or
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	
	Example:
	`Router(config-if-atm-range-pvc)# protocol pppoe group two`
	
	Example:
	
	Example:
	
	Example:
	`Router(config-if-atm-range-pvc)# encapsulation aal5autoppp virtual-template 1 group two`
		Enables PPPoE sessions to be established on a PVC within a range.
		or
		Configures PPPoE autosense.
		Note If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

Step 8	**end** **Example:** `Router(cfg-if-atm-range-pvc)# end`	(Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM VC Class

Perform this task to assign a PPPoE profile to an ATM VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. Do one of the following:
   - **protocol pppoe** [**group** *group-name*]
   -
   - or
   - **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm class1`	Creates an ATM VC class and enters ATM VC class configuration mode. • A VC class can be applied to an ATM interface, subinterface, or VC.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **protocol pppoe** [**group** *group-name*]
	•
	• or
	• **encapsulation aal5autoppp virtual-template** *number* [**group** *group-name*]
	
	Example:
	`Router(config-vc-class)# protocol pppoe group two`
	
	Example:
	
	Example:
	
	Example:
	`Router(config-vc-class)# encapsulation aal5autoppp virtual-template 1 group two`
		Enables PPPoE sessions to be established.
		or
		Configures PPPoE autosense.
		Note If a PPPoE profile is not assigned by using the **group** *group-name* option, the PPPoE sessions will be established with the global PPPoE profile.

Step 5	**end** **Example:** `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.

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.

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*bba-group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group1`	Enters BBA group configuration mode.
Step 4	**mac-address** {**autoselect** | *mac-address*} **Example:** `Router(config-bba-group)# mac-address autoselect`	Selects the MAC address, as follows: • **autoselect** --Automatically selects the MAC address based on the ATM interface address, plus 7. • *mac-address* --Standardized data link layer address having a 48-bit MAC address. Also known as a hardware address, MAC layer address, and physical address. All PPPoEoA sessions use the MAC address specified on the BBA group, which are applied on the VC.
Step 5	**end** **Example:** `Router(config-bba-group)# end`	Exits BBA group configuration mode.

	Command or Action	Purpose
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                                      VA-st
      3      3  000b.fdc9.0001  ATM3/0.1                 1  Vi2.1
PTA
                0008.7c55.a054  VC:  1/50                   UP
LocMAC is burned in mac-address of ATM interface(0008.7c55.a054).
```

Configuring PPPoE Session Recovery After Reload

Perform this task to configure the aggregation device to send PPPoE active discovery terminate (PADT) packets to the CPE device upon receipt of PPPoE packets on "half-active" PPPoE sessions (a PPPoE session that is active on the CPE end only).

If the PPP keepalive mechanism is disabled on a customer premises equipment (CPE) device, a PPP over Ethernet (PPPoE) session will hang indefinitely after an aggregation device reload. The PPPoE Session Recovery After Reload feature enables the aggregation device to attempt to recover PPPoE sessions that failed because of reload by notifying CPE devices about the PPPoE session failures.

The PPPoE protocol relies on the PPP keepalive mechanism to detect link or peer device failures. If PPP detects a failure, it terminates the PPPoE session. If the PPP keepalive mechanism is disabled on a CPE device, the CPE device has no way to detect link or peer device failures over PPPoE connections. When an aggregation 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that will serve as the default profile for any PPPoE port that is not assigned a specific profile.
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, page 28

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. • Enter your password if prompted.
Step 2	**show pppoe session** [**all** | **packets**] **Example:** `Router# show pppoe session all`	Displays information about active PPPoE sessions.
Step 3	**clear pppoe** {**interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] | **rmac** *mac-addr* [**sid** *session-id*] | **all**} **Example:** `Router# clear pppoe interface atm 0/0/0.0`	Terminates PPPoE sessions.
Step 4	**debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}]] **Example:** `Router# debug pppoe events`	Displays debugging information for PPPoE sessions.

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

- Example PPPoE Session Recovery After Reload, page 33

Example PPPoE Profiles Configuration

The following example shows the configuration of three PPPoE profiles: vpn1, vpn2, and a global PPPoE profile. The profiles vpn1 and vpn2 are assigned to PVCs, VC classes, VLANs, and PVC ranges. Any Gigabit Ethernet interface, VLAN, PVC, PVC range, or VC class that is configured for PPPoE but is not assigned either profile vpn1 or vpn (such as VC class class-pppoe-global) will use the global profile.

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
 sessions per-mac limit 2
bba-group pppoe group1
 virtual-template 1
 sessions per-vlan throttle 1 10 50
!
interface GigabitEthernet5/0/0.2
 encapsulation dot1Q 20 second-dot1q 201
 pppoe enable group group1
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
 sessions per-mac limit 1 !
vc-class atm class-pppoe-global
 protocol pppoe
!
vc-class atm class-pppox-auto
 encapsulation aal5autoppp virtual-template 1 group vpn1
!
vc-class atm class-pppoe-1
 protocol pppoe group vpn1
!
vc-class atm class-pppoe-2
 protocol pppoe group vpn2
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
 !
interface ATM1/0.20 multipoint
 class-int class-pppox-auto
 pvc 0/200
  encapsulation aal5autoppp virtual-template 1
 !
 pvc 0/201
 !
 pvc 0/202
  encapsulation aal5autoppp virtual-template 1 group vpn2
 !
 pvc 0/203
  class-vc class-pppoe-global
 !
!
interface gigabitEthernet0/2/3.1
 encapsulation dot1Q 4
 pppoe enable group vpn1
!
interface gigabitEthernet0/2/3.2
```

```
 encapsulation dot1Q 2
 pppoe enable group vpn2
!
interface ATM0/6/0.101 point-to-point
 ip address 10.12.1.63 255.255.255.0
 pvc 0/101
 !
interface ATM0/6/0.102 point-to-point
 ip address 10.12.2.63 255.255.255.0
 pvc 0/102
 !
interface Virtual-Template1
 ip unnumbered loopback 1
 no logging event link-status
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered loopback 1
no logging event link-status
 no keepalive
 peer default ip address pool pool-2
 ppp authentication chap
!
ip local pool pool-1 198.x.1.z 198.x.1.y
ip local pool pool-2 198.x.2.z 198.x.2.y
!
```

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

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

Example Address Autoselect Configured and MAC Address Not Configured

In the following example, address autoselect is configured on the BBA group, and the MAC address is not configured on the ATM interface. The **show pppoe session** command displays the MAC address of the interface, plus 7.

```
bba-group pppoe one
 virtual-template 1
 mac-address autoselect
!
interface ATM3/0
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      5      5  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0008.7c55.a05b  VC:  1/50                   UP
LocMAC = burned in mac-address of ATM interface + 7 (0008.7c55.a05b)
```

Example MAC Address Configured on the ATM Interface

In the following example, neither autoselect nor the MAC address is configured on the BBA group, but the MAC address is configured on the ATM interface, as indicated by the report from the **show pppoe session** command:

```
bba-group pppoe one
 virtual-template 1
interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
protocol pppoe group one
 !
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      7      7  000b.fdc9.0001  ATM0/3/0.1                1  Vi2.1
PTA
                0001.0001.0001  VC:  1/50                   UP
LocMAC = configured mac-address on atm interface(0001.0001.0001).
```

Example MAC Address Configured on the BBA Group

In the following example, the MAC address is configured on the BBA group. The display from the **show pppoe session** command indicates that all PPPoEoA sessions on the ATM interface associated with the BBA group use the same MAC address as specified on the BBA group.

```
bba-group pppoe one
 virtual-template 1
 mac-address 0002.0002.0002
interface ATM0/3/0.0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM0/3/0.1 multipoint
 no ip route-cache
 pvc 1/50
  encapsulation aal5snap
  protocol pppoe group one
Router# show pppoe session
     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA
State
           SID  LocMAC                                      VA-st
      8      8  000b.fdc9.0001  ATM0/3/0.1                 1  Vi2.1
PTA
                0002.0002.0002  VC:  1/50                   UP
LocMac(Mac address of PPPoEoA session) is mac-address specified on bba-group one
(0002.0002.0002)
```

Example PPPoE Session Recovery After Reload

In the following example, the router 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

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

Related Topic	Document Title
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	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

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

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

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

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

Table 3 Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Feature Name	Releases	Feature Information
PPPoE Connection Throttling	Cisco IOS XE Release 2.1	The PPPoE Connection Throttling feature limits PPPoE connection requests to help prevent intentional denial-of-service attacks and unintentional PPP authentication loops. This feature implements session throttling on the PPPoE server to limit the number of PPPoE session requests that can be initiated from a MAC address or virtual circuit during a specified period of time.
PPPoE Server Restructuring and PPPoE Profiles	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
PPPoE VLAN Session Throttling	Cisco IOS XE Release 2.4	This feature allows for PPPoE VLAN Session throttling support.

PPPoE Session Limit Local Override

The PPPoE Session Limit Local Override feature enables the session limit configured locally on the broadband remote access server (BRAS) or L2TP access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is enabled.

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 Table at the end of this document.

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

Information About PPPoE Session Limit Local Override

How PPPoE Session Limit Local Override Works

PPP over Ethernet (PPPoE) session limits are downloaded from the RADIUS server when you enable SSS preauthorization on the LAC using the **subscriber access pppoe pre-authorize nas-port-id**command. By enabling preauthorization, you limit the number of PPPoE sessions on a specific VLAN; that is, the PPPoE per-NAS-port session limit downloaded from the RADIUS server takes precedence over locally configured (port-based) session limits, such as per-VLAN session limits. The following is a sample user profile to configure a session limit through RADIUS:

```
Username=nas_port:10.10.10.10:4/0/0/1.100
```

```
Password = "password1"
cisco-avpair= "pppoe:session-limit=session limit per NAS-port"
```

The PPPoE Session Limit Local Override feature enables the local session limit configured at the BRAS to override the per-NAS-port session limit configured at the RADIUS server when SSS preauthorization is configured.

Note The PPPoE Session Limit Local Override feature is useful only when you have configured SSS preauthorization on the BRAS or LAC.

To enable the PPPoE Session Limit Local Override feature, configure the **sessions pre-auth limit ignore** command under the broadband access (BBA) group associated with the interface. When the PPPoE Session Limit Local Override feature is enabled, the locally configured session limit is applied before PPP is started; that is before the BRAS sends out a PPPoE Active Discovery Offer (PADO) packet to the client, advertising a list of available services.

When preauthorization is configured without the PPPoE Session Limit Local Override feature enabled, the client receives an authentication failure response from the BRAS when there is no session limit downloaded from the RADIUS server and the locally configured session limit is exceeded. The BRAS waits to apply locally configured limits until PPP negotiation is completed. When a call is finally rejected, the client receives the authentication failure response, resulting in session failure, with no ability to distinguish whether the session failure results from a Challenge Handshake Authentication Protocol (CHAP) authentication failure or a PPPoE session limit having been exceeded. The PPPoE Session Limit Local Override feature allows for differentiation between the handling of per-NAS-port failures and session limiting failures.

If you enable the PPPoE Session Limit Local Override feature, but there are no locally configured per-port session limits, then per-NAS-port session limits downloaded from the RADIUS server are applied.

How to Configure PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override

Enable the PPPoE Session Limit Local Override feature to allow the local session limit configured on the BRAS to override the per-NAS-port session limit downloaded from the RADIUS server.

Note If there are no locally configured per-port session limits, then per-NAS port session limits downloaded from the RADIUS server are applied.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **sessions per-vlan limit** *per-vlan-limit*
5. **sessions pre-auth limit ignore**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe test`	Creates a PPPoE profile and enters BBA group configuration mode. • *group-name* --Name of the PPPoE profile.
Step 4	**sessions per-vlan limit** *per-vlan-limit* **Example:** `Router(config-bba-group)# sessions per-vlan limit 3`	Limits the number of PPPoE sessions per VLAN in a PPPoE profile. • *per-vlan-limit* --Maximum number of PPPoE sessions that can be established over an Ethernet VLAN. The default is 100.
Step 5	**sessions pre-auth limit ignore** **Example:** `Router(config-bba-group)# sessions pre-auth limit ignore`	Enables the PPPoE Session Limit Local Override feature. The locally configured limit overrides the per-NAS-port session limit configured at the RADIUS server.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-bba-group)# end`	Exits BBA group configuration mode and returns to privileged EXEC mode.

Configuration Examples for PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override Example

The following example creates a PPPoE group named test, configures a limit of three sessions per VLAN, and enables the PPPoE Session Limit Local Override feature in bba-group configuration mode. The running configuration shows that the **sessions pre-auth limit ignore** command was used to enable this feature.

```
Router(config)# bba-group pppoe test
Router(config-bba-group)# sessions per-vlan limit 3
Router(config-bba-group)# sessions pre-auth limit ignore

.
.
!
bba-group pppoe test
virtual-template 2
sessions per-vlan limit 3
sessions pre-auth limit ignore
!
```

Additional References

The following sections provide references related to the PPPoE Session Limit Local Override feature.

Related Documents

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* • 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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for PPPoE Session Limit Local Override

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

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

Table 4 Feature Information for PPPoE Session Limit Local Override

Feature Name	Releases	Feature Information
PPPoE--Session Limit Local Override	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. This feature enables the session limit configured locally on the broadband remote access server (BRAS) or L2TP access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is enabled. The following commands were introduced or modified: **sessions pre-auth limit ignore**.

PPPoE Circuit-Id Tag Processing

The PPPoE Circuit-Id Tag Processing feature provides a way to extract a Circuit-Id tag from the digital subscriber line (DSL) as an identifier for the authentication, authorization, and accounting (AAA) access request on a Fast Ethernet or Gigabit Ethernet interface, thereby simulating ATM-based Broadband access, but using cost-effective Fast Ethernet or Gigabit Ethernet instead. The tag is useful for troubleshooting the network, and is also used in RADIUS authentication and accounting processes.

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 Table at the end of this document.

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

Prerequisites for the PPPoE Circuit-Id Tag Processing Feature

It is recommended that you be familiar with RFC 2516 before configuring this feature. See the Prerequisites for the PPPoE Circuit-Id Tag Processing Feature, page 43 for a pointer to this standard.

Information About the PPPoE Circuit-Id Tag Processing Feature

Differences Between ATM- and Fast or Gigabit Ethernet-Based Broadband Access Networks

Broadband digital subscriber line multiplexer (DSLAM) and Broadband Remote Access Server (BRAS) vendors see a need to provide Fast or Gigabit Ethernet-based networks as an alternative to an ATM access network, with a DSLAM bridging the ATM-DSL local loop to the Fast or Gigabit Ethernet-based access network and allowing Fast or Gigabit Ethernet-based connectivity to the BRAS. But in an Fast or Gigabit Ethernet access network, there is no unique mapping between the subscriber Line-Id and the interface, as is found in an ATM-based network. In an ATM-based network, the ATM VC is associated to a subscriber line.

During the authentication phase that initiates the PPP access and AAA accounting requests, the BRAS includes a NAS-Port-Id attribute in RADIUS authentication packets, if the feature "TAL based on the NAS-Port-Id" feature is configured. This attribute identifies the DSL line for the subscriber. See Configuring BRAS to Include a NAS-Port-Id Attribute Example, page 50 for an example.

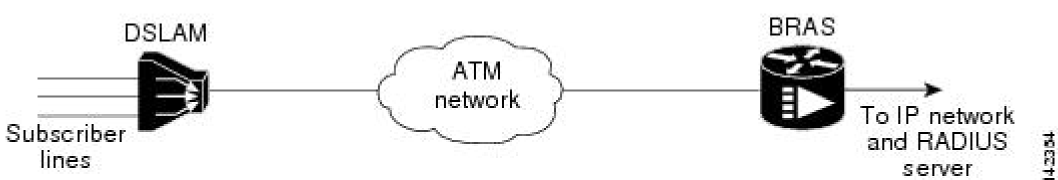
DSL Forum 2004-71 Solution

To apply the same subscriber mapping capability to Fast or Gigabit Ethernet interfaces that is possible on ATM interfaces, DSL Forum 2004-71 proposes a solution whereby the DSLAM sends the DSL Line-Id in the PPP over Ethernet (PPPoE) discovery phase. This method provides a way for a PPPoE server acting as a BRAS to extract the Line-Id tag and use the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests. The PPPoE Circuit-Id Tag Processing feature makes use of the proposed DSL Forum 2004-71 method and allows the BRAS to detect the presence of the subscriber Circuit-Id tag inserted by the DSLAM during the PPPoE discovery phase. The BRAS will send this tag as a NAS-Port-Id attribute in PPP authentication and AAA accounting requests. The tag is useful in troubleshooting the Ethernet network, and it is also used in RADIUS authentication and accounting processes.

Approach for a Circuit-Id Tag in Ethernet-Based Broadband Access Networks

Traditional ATM-based DSL broadband access networks have the topology shown in the figure below.

Figure 1 ATM-Based DSL Broadband Access Network

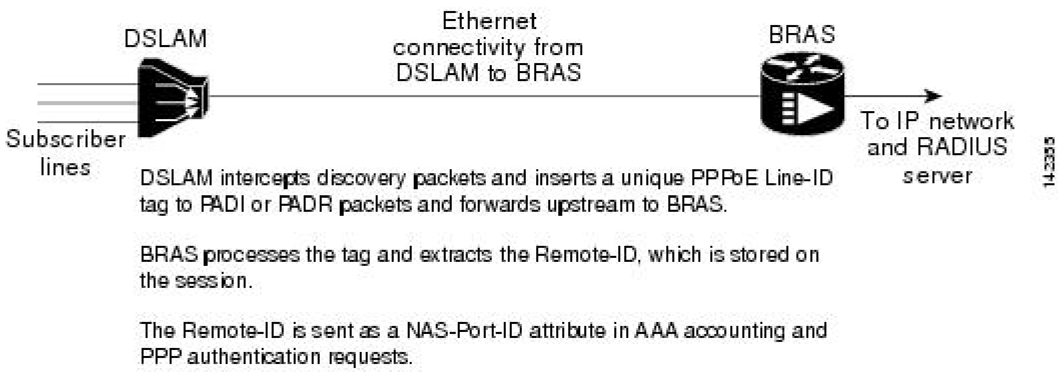


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM VC used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-Id for use in RADIUS packets.

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 the figure below. The DSLAM forwards these packets to the BRAS after the insertion. The tag contains the circuit-id of the DSL line on which the PADI or PADR packet was received, in the access node where the intermediate agent resides.

Figure 2 PPPoE Circuit-Id Tag Processing Solution



When the **vendor-tag circuit-id service** command is configured in BBA (broadband access) group configuration mode, the BRAS processes the received PPPoE Vendor-Specific tag in the PADR packet and extracts the Circuit-Id field, which is sent to the remote AAA server as the NAS-Port-Id attribute (RADIUS attribute 87) in RADIUS access and accounting requests. When the **radius-server attribute nas-port format d** global configuration command is also configured on the BRAS, the Acct-Session-Id attribute will contain the information about the incoming access interface, where discovery frames are received, and about the session being established.

Outgoing PAD Offer and Session-confirmation (PADO and PADS) packets from the BRAS will have the DSLAM-inserted Circuit-Id tag. DSLAM should strip the tag out of PADO and PADS packets. If the DSLAM cannot strip off the tag, the BRAS should remove it before sending the packets out, and this is accomplished using the **vendor-tag circuit-id strip** BBA group configuration mode command.

Benefits of the PPPoE Circuit-Id Tag Processing Feature

The shift towards Fast or Gigabit Ethernet-based DSLAMs offers the following benefits:

- Ability to use simpler and lower cost provisioning options for DSL subscribers over an Fast or Gigabit Ethernet-based backhaul network rather than on an ATM-based network.
- Ability to use higher bandwidth connectivity options available from Fast or Gigabit Ethernet not possible on ATM.
- Ability to upgrade to next-generation DSLAMs with quality of service (QoS), and support for higher bandwidth, asymmetric dual latency modems such as the ADSL2.
- Ability to inject high-bandwidth content such as video in an Ethernet network.

How to Configure the PPPoE Circuit-Id Tag Processing Feature

Configuring the PPPoE Circuit-Id Tag Processing Feature

This section describes how to configure an Fast or Gigabit Ethernet-based access network on a Cisco BRAS. The extracted Circuit-Id tag (see Information About the PPPoE Circuit-Id Tag Processing Feature, page 43) is sent in the following RADIUS syntax, as recommended by the DSL Forum:

"Access-Node-Identifier eth *slot*/*port* [**:***vlan-tag*]"

The Access-Node-Identifier is a unique subscriber identifier or telephone number text string entered without spaces. Per DSL-Forum 2004-71, the maximum length supported for the tag is 48 bytes. The BRAS copies the entire tag into the NAS-Port-Id and sends it to the AAA server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **bba-group pppoe** *group-name*
5. **vendor-tag circuit-id service**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**radius-server attribute nas-port format d** **Example:** `Router(config)# radius-server attribute nas-port format d`	(Optional) Selects the PPPoE extended NAS-Port format used for RADIUS access and accounting. • Configure this command so that the Acct-Session-Id attribute, as displayed in the **debug radius** command, will contain the information about the incoming access interface, where discovery frames are received, and about the session being established. See the Displaying the Session Activity Log, page 48 and Configuring PPPoE Circuit-Id Tag Processing Example, page 50 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

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**vendor-tag strip** **Example:** `Router(config-bba-group)# vendor-tag strip`	Enables the BRAS to strip off incoming Vendor-Specific Circuit-Id tags from outgoing PADO and PADS packets.

Displaying the Session Activity Log

When the **radius-server attribute nas-port format d** global configuration command is added to the PPPoE Circuit-Id Tag Processing feature configuration on the BRAS (see the Configuring PPPoE Circuit-Id Tag Processing Example, page 50 for an example), the report from the **debug radius** privileged EXEC command will include information about the incoming access interface, where discovery frames are received, and about the session being established in PPPoE extended NAS-Port format (format d).

Enable the **debug radius** command to display a report of session activity. In the example shown in this section:

- The acct_session_id is 79 or 4F in hexadecimal format.
- In the message "Acct-session-id pre-pended with Nas Port = 0/0/0/200," the interface on which the PPPoE discovery frames arrived is FastEthernet0/0.200. The 0/0/0 is Cisco format for slot/subslot/port.
- The Acct-Session-Id vendor-specific attribute 44 contains the string "0/0/0/200_0000004F," which is a combination of the ingress interface and the session identifier.

Note Strings of interest in the **debug radius** output log are presented in bold text for example purposes only.

```
Router# debug radius
```

```
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS/ENCODE(0000003F): acct_session_id: 79
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server
172.20.164.143
02:10:49: RADIUS(0000003F): Send Access-Request to 172.20.164.143:1645 id 1645/65, len 98
02:10:49: RADIUS:  authenticator 1C 9E B0 A2 82 51 C1 79 - FE 24 F4 D1 2F 84 F5 79
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                       [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  CHAP-Password       [3]   19  *
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                  [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS: Received from id 1645/65 172.20.164.143:1645, Access-Accept, len 32
02:10:49: RADIUS:  authenticator 06 45 84 1B 27 1F A5 C3 - C3 C9 69 6E B9 C0 6F 94
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                       [1]
02:10:49: RADIUS(0000003F): Received from id 1645/65
02:10:49: [62]PPPoE 65: State LCP_NEGOTIATION    Event PPP_LOCAL
02:10:49: PPPoE 65/SB: Sent vtemplate request on base Vi2
02:10:49: [62]PPPoE 65: State VACCESS_REQUESTED    Event VA_RESP
02:10:49: [62]PPPoE 65: Vi2.1 interface obtained
02:10:49: [62]PPPoE 65: State PTA_BINDING    Event STAT_BIND
02:10:49: [62]PPPoE 65: data path set to Virtual Acess
02:10:49: [62]PPPoE 65: Connected PTA
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: [62]PPPoE 65: AAA get dynamic attrs
02:10:49: RADIUS/ENCODE(0000003F):Orig. component type = PPoE
02:10:49: RADIUS/ENCODE(0000003F): Acct-session-id pre-pended with Nas Port = 0/0/0/200
02:10:49: RADIUS(0000003F): Config NAS IP: 0.0.0.0
02:10:49: RADIUS(0000003F): sending
02:10:49: RADIUS/ENCODE: Best Local IP-Address 10.0.58.141 for Radius-Server
172.20.164.143
02:10:49: RADIUS(0000003F): Send Accounting-Request to 172.20.164.143:1646 id 1 646/42,
len 117
02:10:49: RADIUS:  authenticator 57 24 38 1A A3 09 62 42 - 55 2F 41 71 38 E1 CC 24
02:10:49: RADIUS:  Acct-Session-Id     [44]  20  "0/0/0/200_0000004F"
02:10:49: RADIUS:  Framed-Protocol     [7]   6 PPP                       [1]
02:10:49: RADIUS:  User-Name           [1]   7   "peer1"
02:10:49: RADIUS:  Acct-Authentic      [45]  6 RADIUS                    [1]
02:10:49: RADIUS:  Acct-Status-Type    [40]  6 Start                     [1]
02:10:49: RADIUS:  NAS-Port-Type       [61]  6 Ethernet                  [15]
02:10:49: RADIUS:  NAS-Port            [5]   6   200
02:10:49: RADIUS:  NAS-Port-Id         [87]  22  "FastEthernet6/0.200:"
02:10:49: RADIUS:  Service-Type        [6]   6 Framed                    [2]
02:10:49: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.141
02:10:49: RADIUS:  Acct-Delay-Time     [41]  6   0
02:10:49: RADIUS: Received from id 1646/42 172.20.164.143:1646, Accounting-resp onse, len
20
02:10:49: RADIUS:  authenticator 34 84 7E B2 F4 40 B2 7C - C5 B2 4E 98 78 03 8B C0
```

Configuration Examples for the PPPoE Circuit-Id Tag Processing Feature

Configuring PPPoE Circuit-Id Tag Processing Example

In the following example, outgoing PADO and PADS packets will retain the incoming Vendor-Specific Circuit-Id tag:

```
radius-server attribute nas-port format d
!
bba-group pppoe pppoe-group
 sessions per-mac limit 50
 vendor-tag circuit-id service
!
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

Configuring BRAS to Include a NAS-Port-Id Attribute Example

In the following example, the feature TAL based on the NAS-Port-Id is configured. This configuration ensures that a NAS-Port-Id attribute is included in RADIUS authentication packets during the authentication phase to initiate PPP access and AAA accounting requests.

```
radius-server attribute nas-port
policy-map type control test
 class type control always event session-start
 1 authorize identifier nas-port
```

Removing the PPPoE Circuit-Id Tag Example

In the following example, the BRAS will strip off incoming Vendor-Specific Circuit-Id tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service
 vendor-tag strip
interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-group
```

Additional References

The following sections provide references related to the PPPoE Circuit-Id Tag Processing feature.

Related Documents

Related Topic	Document Title
Configuring Broadband and DSL	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
RADIUS attributes	*Cisco IOS XE Security Configuration Guide*
DSL Forum Line-Id tag solution	Broadband Forum

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE)

Technical Assistance

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

Feature Information for PPPoE Circuit-Id Tag Processing

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

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

Table 5 Feature Information for PPPoE Circuit-Id Tag Processing

Feature Name	Releases	Feature Information
PPPoE Circuit-Id Tag Processing	Cisco IOS XE Release 2.1.	The PPPoE Circuit-Id Tag Processing feature provides a way to extract a Circuit-Id tag from the DSL as an identifier for the AAA access request on an Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Ethernet instead. The tag is useful for troubleshooting the network, and is also used in RADIUS authentication and accounting processes. This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature was integrated into Cisco IOS XE Release 2.3.1. The following commands were introduced or modified: **vendor-tag circuit-id service**, **vendor-tag strip**.

Configuring PPP over Ethernet Session Limit Support

This module provides information on how to limit the number of PPP over Ethernet (PPPoE) sessions that can be created on a router or on a Gigabit Ethernet interface for configuration.

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 Table at the end of this document.

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

Information About Configuring PPP over Ethernet Session Limit Support

Benefits of Configuring PPP over Ethernet Session Limit Support

- The PPPoE Session Limit Support feature prevents the router from using too much memory for virtual access by limiting the number of PPPoE sessions that can be created on a router or on all Ethernet interfaces and subinterfaces as well as ATM interfaces and subinterfaces.
- The SNMP Enhancements for ASR 1000 feature enhances Cisco ASR 1000 Aggregation Series Router to count the PPPoE sessions in PTA, FWDED, and TRANS state for a particular physical

interface, and the total number of sessions that exist in a physical interface. Provision for using a system-wide threshold trap and per-physical threshold trap is provided through SNMP. These functionalities enable users to retrieve the total number of sessions and per-interface session-loss threshold value.

Trap Generation

In scenarios where you must deploy ASR 1000 Series Routers with one physical port mapped to one DSLAM and if the total number of sessions for the DSLAM falls below the threshold value on a physical interface, due to a loss of high number of sessions, a notification trap is generated. You can use these traps to investigate the issue and take immediate actions.

When the number of active sessions falls below the threshold value, only one trap is generated. Further traps are not sent even if the number of sessions continue to decrease. The next set of traps are sent only if the number of sessions rise above the configured threshold value and fall. This criterion is applicable to both global and per-interface traps.

When threshold values are configured in both global and per-interface configuration modes, then both the threshold values are monitored separately. Traps are sent when the session count falls below the threshold value either in global configuration mode or in per-interface configuration mode.

How to Configure PPP over Ethernet Session Limit Support

Specifying the Maximum Number of PPPoE Sessions on a Router

Perform this task to specify the maximum number of PPPoE sessions that can be created on a router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id*]
7. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
8. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Configures a broadband aggregation (BBA) group to be used to establish PPPoE sessions and enters BBA group configuration mode. • *name* --Name of the BBA group. You can have multiple BBA groups. • **global** -- Specifies the PPPoE profile that serves as the default profile for any PPPoE port (Gigabit Ethernet interface or VLAN) that has not been assigned a specific PPPoE profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template that will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 1000`	(Optional) Configures the maximum number of PPPoE sessions allowed per MAC session limit in a PPPoE profile. The default MAC session limit is 100.
Step 6	**sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id*] **Example:** `Router(config-bba-group)# session per-vlan limit 4000 inner 3500`	(Optional) Sets the session limit for the inner VLAN on QinQ subinterface. The default session limit is 100. **Note** The per-VLAN limit is only applicable to Gigabit Ethernet subinterfaces (802.1q VLANs).

	Command or Action	Purpose
Step 7	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit 2000`	(Optional) Sets the maximum number of PPPoE sessions allowed per VC session limit in a PPPoE profile. The default session limit is 100. **Note** The per-VC limit is applicable only to ATM interfaces and subinterfaces.
Step 8	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 32000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated. **Note** This command applies only to the global profile.
Step 9	**exit** **Example:** `Router(config-bba-group)# exit`	Returns to global configuration mode.

Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface

Perform this task to specify the maximum number of PPPoE sessions that can be created on a Gigabit Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** {**GigabitEthernet** | **tenGigabitEthernet**} *slot* / *subslot* / *port*[**.** *subinterface*]
4. **pppoe enable** [**group** *group-name*]
5. **pppoe max-sessions** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** {**GigabitEthernet** | **tenGigabitEthernet**} *slot* / *subslot* / *port*[**.** *subinterface*] **Example:** `Router(config)# interface GigabitEthernet0/0/1`	Specifies a Gigabit Ethernet interface and enters interface configuration mode.
Step 4	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-if)# pppoe enable group one`	Enables PPPoE sessions on a Gigabit Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface through the use of the **group** *group-name* option, the interface will use the global PPPoE profile.
Step 5	**pppoe max-sessions** *number* **Example:** `Router(config-if)# pppoe max-sessions 10`	Specifies the maximum number of PPPoE sessions permitted on the interface or subinterface.
Step 6	**end** **Example:** `Router(config-if)# end`	(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuring System-Wide Threshold Parameters

Performthis task to configure the system-wide threshold parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group ppp oe globa** l
4. **sessions threshold** *number*
5. **exit**
6. **interface** type *number*
7. **pppoe-sessions threshold** *number*
8. **end**
9. **show pppoe summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router> configure terminal`	Enters global configuration mode.
Step 3	**bba-group ppp oe globa** l **Example:** `Router(config)# bba-group pppoe global`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**sessions threshold** *number* **Example:** `Router(config-bba-group)# sessions threshold 1000`	Configures the global threshold value.
Step 5	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
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

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	Cisco IOS Master Commands List, All Releases
Broadband and DSL commands	*Cisco IOS Broadband and DSL Command Reference*

Related Topic	Document Title
Broadband access aggregation of PPPoE sessions	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Configuring PPP over Ethernet Session Limit Support

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

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

Table 6 Feature Information for Providing PPP over Ethernet Session Limit Support

Feature Name	Releases	Feature Information
PPP over Ethernet Session Limit Support	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.4	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The PPPoE Session Limit Support feature enables you to limit the number of PPPoE sessions that can be created on a router or on a Gigabit Ethernet interface for configuration. This feature was integrated into Cisco IOS XE Release 2.4.
SNMP Enhancements for ASR 1000	Cisco IOS XE Release 3.2S	The SNMP Enhancements for ASR 1000 feature enhances Cisco ASR 1000 Aggregation Series Routers to provide the count of the PPPOE sessions in PTA, Forwarded, and TRANS state for a particular physical interface, and the total count of sessions that exist in a physical interface. This feature was introduced in Cisco IOS XE 3.2S. The following commands were introduced or modified: **pppoe-sessions threshold**, **sessions threshold**.

PPP-Max-Payload and IWF PPPoE Tag Support

The PPP-Max-Payload and IWF PPPoE Tag Support feature enables the PPP over Ethernet (PPPoE) component to process the PPP-Max-Payload and Interworking Functionality (IWF) PPPoE tags in the PPPoE discovery frame:

- The **tag ppp-max-payload** command allows PPPoE peers to negotiate PPP maximum receive units (MRUs) greater than 1492 octets if the underlying network supports a maximum transmission unit (MTU) size greater than 1500 octets.
- The IWF PPPoE tag allows the Broadband Remote Access Server (BRAS) to distinguish the IWF PPPoE from the regular PPPoE sessions to overcome the per-MAC session limit put on the BRAS as a protection from denial of service (DOS) attacks sourced from the same MAC address.

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 Table at the end of this document.

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

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

Accommodating an MTU MRU Greater than 1492 in PPPoE

Per the RFC, "Accommodating an MTU/MRU Greater than 1492 in PPPoE," PPPoE peers can negotiate only MRUs with a maximum of 1492 octets so that the PPPoE header and PPP protocol ID can be inserted in the PPPoE session data packet. The maximum for an Ethernet payload is 1500 octets.

RFC 2516 defines a new tag to allow PPPoE peers to negotiate PPP MRU greater than 1492 if the underlying networks can support an Ethernet payload of greater than 1500 bytes. To enable processing of this new tag, a command has been defined in the Cisco IOS command-line interface as **tag ppp-max-payload.**The PPP-Max-Payload and IWF PPPoE Tag Support feature enhances the PPPoE component so the **tag ppp-max-payload**command can process the new tag to influence the Link Control Protocol (LCP) MRU negotiations for the PPP session based on the MRU value specified in the tag from the PPPoE client.

Interworking Functionality

The DSL Forum defined IWF to define the process for conversion of PPP over ATM (PPPoA) sessions to PPPoE sessions at the digital subscriber line access multiplexer (DSLAM) to the BRAS. This functionality was defined to help the migration of DSLAM networks from ATM to Ethernet media. So, essentially, the PPPoA session comes in to the DSLAM over ATM and is converted to a PPPoE session at the DSLAM, which is then connected to the BRAS as a PPPoE session. Each PPPoA session is mapped to a corresponding PPPoE session.

Typically, the BRAS is configured to limit PPPoE sessions originating from the same MAC address to protect itself from a DOS attack. This presents a problem for IWF PPPoE sessions because all PPPoE sessions originate from the same MAC address DSLAM. To overcome this issue, the IWF PPPoE tag is inserted at the DSLAM and read by the BRAS to distinguish the IWF PPPoE session from the regular PPPoE session during the PPPoE discovery frames.

For more information about this subject, refer to the DSL Forum Technical Report 101, "Migration to Ethernet-Based DSL Aggregation."

How to Configure PPP-Max-Payload and IWF PPPoE Tag Support

- Enabling PPP-Max-Payload and IWF PPPoE Tag Support, page 66
- Disabling PPP-Max-Payload and IWF PPPoE Tag Support, page 69

Enabling PPP-Max-Payload and IWF PPPoE Tag Support

To enable the PPP-Max-Payload and IWF PPPoE Tag Support feature, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**]
6. **sessions per-mac iwf limit** *per-mac-limit*
7. **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot* **/subslot/** *port[subinterface]*
8. **pppoe enable [group** *group-name]*
9. **virtual-template** *template-number*
10. **ppp lcp echo mru verify** [**minimum** *value*]
11. **end**
12. **show pppoe session** [**all**| **packets**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.

	Command or Action	Purpose
Step 5	**tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**] **Example:** `Router(config-bba-group)# tag ppp-max-payload minimum 1200 maximum 3000`	Specifies a range for the ppp-max payload tag value that will be accepted by the BRAS. • Default values are 1492 for the minimum and 1500 for the maximum. • The ppp-max-payload tag value accepted from the client cannot exceed the physical interface value for MTU minus 8.
Step 6	**sessions per-mac iwf limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac iwf limit 200`	Specifies a limit for IWF-specific sessions per MAC address (separate from session limits that are not IWF-specific). • If this command is not entered, the normal MAC-address session limit is applied to IWF sessions. • The *per-mac-limit* argument specifies the allowable number of IWF sessions. The default is 100.
Step 7	**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot* **/subslot/** *port[subinterface]* **Example:** `Router(config-bba-group)# interface gigabitethernet 0/0/0`	Enters interface configuration mode for a Gigabit Ethernet interface.
Step 8	**pppoe enable [group** *group-name]* **Example:** `Router(config-if)# pppoe enable group 1`	Enables PPPoE sessions on an Ethernet interface or subinterface.
Step 9	**virtual-template** *template-number* **Example:** `Router(config-if)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.
Step 10	**ppp lcp echo mru verify** [**minimum** *value*] **Example:** `Router(config-if)# ppp lcp echo mru verify minimum 1304`	Verifies the negotiated MRU and adjusts the PPP virtual access interface MTU for troubleshooting purposes. • If the optional **minimum** keyword is entered, the *value* can be from 64 to 1500. • If the verification of minimum MTU succeeds, the PPP connection's interface MTU is set to that value. This reset is useful when you troubleshoot and need to adjust the sessions according to underlying physical network capability. After this command is configured, IP Control Protocol (IPCP) is delayed until verification of the MTU is completed at the LCP.

	Command or Action	Purpose
Step 11	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 12	**show pppoe session** [**all**| **packets**] **Example:** `Router# show pppoe session all`	Verifies the configuration and displays session information. • **all** --Displays output indicating if a session is IWF-specific or if the PPP-Max-Payload tag is in the discovery frame and accepted. • **packets** --Displays packet statistics for the PPPoE session.

Disabling PPP-Max-Payload and IWF PPPoE Tag Support

The **tag ppp-max-payload** command adjusts PPP MTU of the PPPoE session above the default maximum limit of 1492 bytes. But MTU values greater than 1492 can only be supported (with PPPoE) if the underlying Ethernet network supports these larger frames. Not all Ethernet networks support higher values. If your network does not support values higher than the default maximum, you should disable the PPP-Max-Payload and IWF PPPoE Tag Support feature by performing this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **tag ppp-max-payload deny**

DETAILED STEPS

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

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

Configuration Examples for PPP-Max Payload and IWF PPPoE Tag Support

This section provides a sample configuration showing the PPP-Max-Payload and IWF PPPoE Tag Support feature enabled and a configuration in which the effects of this feature are disabled:

- PPP-Max-Payload and IWF PPPoE Tag Support Enabled Example, page 70
- PPP-Max-Payload and IWF PPPoE Tag Support Disabled Example, page 70

PPP-Max-Payload and IWF PPPoE Tag Support Enabled Example

The following configuration example shows the PPP-Max-Payload and IWF PPPoE Tag Support enabled to accept PPP-Max-Payload tag values from 1492 to 1892, limits the number of sessions per MAC address to 2000 when the IWF is present, and verifies that the PPP session can accept 1500-byte packets in both directions:

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload minimum 1492 maximum 1892
 sessions per-mac limit 1
 sessions per-mac iwf limit 2000
 ppp lcp echo mru verify
!
 interface Virtual-Template 1
!
```

PPP-Max-Payload and IWF PPPoE Tag Support Disabled Example

The following configuration example disables the effect of the **tag ppp-max-payload** command:

```
bba-group pppoe global
 virtual-template 1
 tag ppp-max-payload deny
```

Additional References

The following sections provide references related to the PPP-Max-Payload and IWF PPPoE Tag Support feature.

Related Documents

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* • Cisco IOS Master Command List, All Releases

Standards

Standard	Title
DSL Forum Technical Report 101	Migration to Ethernet-Based DSL Aggregation

MIBs

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

RFCs

RFCs	Title
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
Draft RFC document	Accommodating an MTU/MRU Greater than 1492 in PPPoE

Technical Assistance

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

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

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

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

Table 7 Feature Information for PPP-Max-Payload and IWF PPPoE Tag Support

Feature Name	Releases	Feature Information
PPP-Max Payload and IWF PPPoE Tag Support	Cisco IOS XE Release 2.3	This feature was introduced on Cisco ASR 1000 Series Routers. This feature enables the PPP over Ethernet (PPPoE) component to process the PPP-Max-Payload and Interworking Functionality (IWF) PPPoE tags in the PPPoE discovery frame. The following commands were introduced or modified: **ppp lcp echo mru verify**, **sessions per-mac iwf limit**, **show pppoe session**, **tag ppp-max-payload**.

PPPoE QinQ Support

The PPPoE QinQ Support feature installed at a subinterface level preserves VLAN IDs and segregates the traffic in different customer VLANs. Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs.

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 Table at the end of this document.

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

Prerequisites for PPPoE QinQ Support

- You have checked Cisco Feature Navigator at http://www.cisco.com/go/cfn to verify that your Cisco device and Cisco IOS XE release support this feature.
- You must be connected to an Ethernet device that supports double VLAN tag imposition/disposition or switching.

Information About PPPoE QinQ Support

PPPoE QinQ Support on Subinterfaces

The PPPoE QinQ Support feature adds another layer of IEEE 802.1Q tag (called "metro tag" or "PE-VLAN") to the 802.1Q tagged packets that enter the network. The purpose is to expand the VLAN space by tagging the tagged packets, thus producing a "double-tagged" frame. The expanded VLAN space allows service providers to offer assorted services on different VLANs. For example, certain customers can be provided Internet access on specific VLANs while other customers receive different services on other VLANs.

Generally the service provider's customers require a range of VLANs to handle multiple applications. Service providers can allow their customers to use this feature to safely assign their own VLAN IDs on subinterfaces because these subinterface VLAN IDs are encapsulated within a service provider-designated VLAN ID for that customer. Therefore there is no overlap of VLAN IDs among customers, nor does traffic from different customers become mixed. The double-tagged frame is "terminated" or assigned on a subinterface through use of an expanded **encapsulation dot1q** command that specifies the two VLAN ID tags (outer VLAN ID and inner VLAN ID) terminated on the subinterface. See GUID-4F84754A-0E3E-48CF-BA54-330C5DB273467.

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.

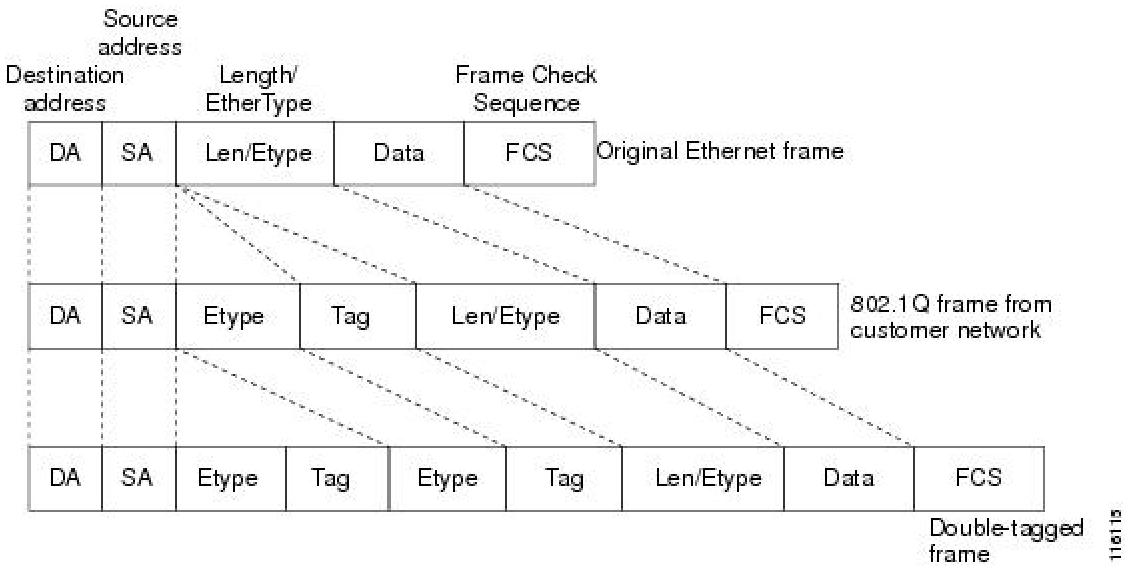
A primary consideration is whether you assign ambiguous or unambiguous subinterfaces for the inner VLAN ID. See the Unambiguous and Ambiguous Subinterfaces, page 78.

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.

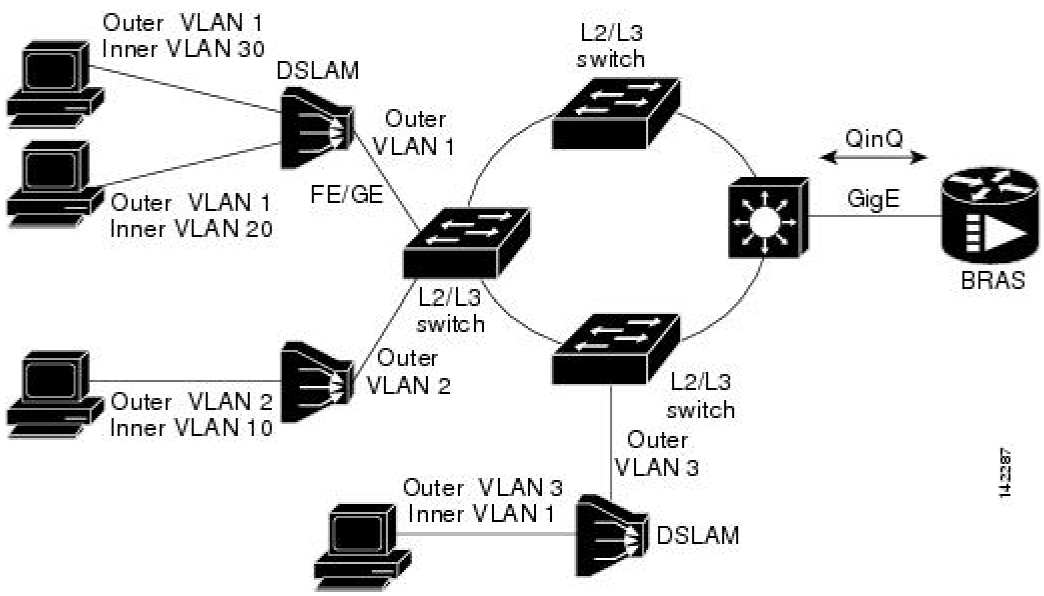
Figure 3 *Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames*



Broadband Ethernet-Based DSLAM Model of QinQ VLANs

For the emerging broadband Ethernet-based DSLAM market, the Cisco ASR 1000 Series Routers support QinQ encapsulation. With the Ethernet-based DSLAM model shown in the figure below, customers typically get their own VLAN; all these VLANs are aggregated on a DSLAM.

Figure 4 *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 Broadband Ethernet-Based DSLAM Model of QinQ VLANs, page 77.

QinQ encapsulation supports configurable outer tag Ethertype. The configurable Ethertype field values are 0x8100 (default), 0x9100, 0x9200, and 0x8848. See the figure below.

Figure 5 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, page 84 for an example of how VLAN IDs are assigned to subinterfaces, and for a detailed example of how the **any** keyword is used on ambiguous subinterfaces.

Note

The **any** keyword in the **second-dot1q**keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. Therefore, multiple values and ranges for the inner VLAN ID are not supported on IPoQinQ.

How to Configure PPPoE QinQ Support

Configuring the Interfaces for PPPoE QinQ Support

Perform this task to configure the main interface used for the QinQ double tagging and to configure the subinterfaces. An optional step in this task shows you how to configure the Ethertype field to be 0x9100 for the outer VLAN tag, if that is required. After the subinterface is defined, the 802.1Q encapsulation is configured to use the double tagging.

- PPPoE or IP is already configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* /*subslot*/*port*
4. **dot1q tunneling ethertype** *ethertype*
5. **exit**
6. **interface** *type slot* /*subslot*/*port*[.*subinterface*]
7. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*| *vlan-id* **-** *vlan-id*[**,** *vlan-id* **-** *vlan-id*]}
8. **pppoe enable** [**group** *group-name*]
9. **ip address** *ip-address mask* [**secondary**]
10. **exit**
11. Repeat Step 6 to configure another subinterface.
12. Repeat Step 7, Step 8, and Step 9, as required, to specify the VLAN tags to be terminated on the subinterface.
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* /*subslot*/*port* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**dot1q tunneling ethertype** *ethertype* **Example:** `Router(config-if)# dot1q tunneling ethertype 0x9100`	(Optional) Defines the Ethertype field type used by peer devices when implementing QinQ VLAN tagging. • Use this command if the Ethertype of peer devices is 0x9100 or 0x9200.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.
Step 6	**interface** *type slot* /*subslot*/*port*[.*subinterface*] **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.1`	Configures a subinterface and enters subinterface configuration mode.

	Command or Action	Purpose
Step 7	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*| *vlan-id* **-** *vlan-id*[**,** *vlan-id* **-** *vlan-id*]} **Example:** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	(Required) Enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. • Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface. • In this example, an unambiguous QinQ subinterface is configured because only one inner VLAN ID is specified. • QinQ frames with an outer VLAN ID of 100 and an inner VLAN ID of 200 will be terminated.
Step 8	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group vpn1`	(Optional) Enables PPPoE sessions on a subinterface. • The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface. **Note** This step is required only for PPPoEoQinQ.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 192.168.1.2 255.255.255.0`	(Optional) Sets a primary or secondary IP address for a subinterface. • The example enables IP on the subinterface specified by the IP address, 192.168.1.2, and mask, 255.255.255.0. **Note** This step is required only for IPoQinQ.
Step 10	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.
Step 11	Repeat Step 6 to configure another subinterface. **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.2`	(Optional) Configures a subinterface and enters subinterface configuration mode.

	Command or Action	Purpose

Step 12	Repeat Step 7, Step 8, and Step 9, as required, to specify the VLAN tags to be terminated on the subinterface.
	
	Example:
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600`
	
	Example:
	`Router(config-subif)# pppoe enable group vpn1`
	
	Example:
	`Router(config-subif)# ip address 192.168.1.2 255.255.255.0`
		Specifies the VLAN tags to be terminated on the subinterface, to enable PPPoE sessions or IP on the subinterface.
		• Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface.
		• In the example, an ambiguous QinQ subinterface is configured because a range of inner VLAN IDs is specified.
		• QinQ frames with an outer VLAN ID of 100 and an inner VLAN ID in the range of 100 to 199 or 201 to 600 will be terminated.
		• Step 7 enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
		• Step 8 enables PPPoE sessions on the subinterface. The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface.
		• Step 9 enables IP on a subinterface specified by the IP address and mask. The example enables IP on the subinterface specified by the IP address, 192.168.1.2, and mask, 255.255.255.0.
		Note Both PPPoE sessions and IP can be enabled on a subinterface.

Step 13	**end** **Example:** `Router(config-subif)# end`	Exits subinterface configuration mode and returns to privileged EXEC mode.

Verifying the PPPoE QinQ Support

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

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show vlans dot1q** [**internal** | *interface-type interface-number.subinterface-number*[**detail**] | *outer-id*[*interface-type interface-number* | **second-dot1q** [*inner-id*| **any**]] [**detail]**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show running-config**

Use this command to show the currently running configuration on the device. You can use delimiting characters to display only the relevant parts of the configuration.

The following output shows the currently running PPPoEoQinQ and IPoQinQ configurations:

Example:

```
Router# show running-config
interface GigabitEthernet0/0/0.201
 encapsulation dot1Q 201
 ip address 10.7.7.5 255.255.255.252
!
interface GigabitEthernet0/0/0.401
 encapsulation dot1Q 401
 ip address 10.7.7.13 255.255.255.252
!
interface GigabitEthernet0/0/0.201999
 encapsulation dot1Q 201 second-dot1q any
 pppoe enable
!
interface GigabitEthernet0/0/0.2012001
 encapsulation dot1Q 201 second-dot1q 2001
 ip address 10.8.8.9 255.255.255.252
!
interface GigabitEthernet0/0/0.2012002
 encapsulation dot1Q 201 second-dot1q 2002
 ip address 10.8.8.13 255.255.255.252
 pppoe enable
!
interface GigabitEthernet0/0/0.4019999
 encapsulation dot1Q 401 second-dot1q 100-900,1001-2000
 pppoe enable
!
interface GigabitEthernet1/0/0.101
 encapsulation dot1Q 101
 ip address 10.7.7.1 255.255.255.252
!
interface GigabitEthernet1/0/0.301
 encapsulation dot1Q 301
 ip address 10.7.7.9 255.255.255.252
!
interface GigabitEthernet1/0/0.301999
 encapsulation dot1Q 301 second-dot1q any
 pppoe enable
!
interface GigabitEthernet1/0/0.1011001
 encapsulation dot1Q 101 second-dot1q 1001
 ip address 10.8.8.1 255.255.255.252
!
interface GigabitEthernet1/0/0.1011002
 encapsulation dot1Q 101 second-dot1q 1002
 ip address 10.8.8.5 255.255.255.252
!
interface GigabitEthernet1/0/0.1019999
 encapsulation dot1Q 101 second-dot1q 1-1000,1003-2000
 pppoe enable
```

Step 3 **show vlans dot1q** [**internal** | *interface-type interface-number*.*subinterface-number*[**detail**] | *outer-id*[*interface-type interface-number* | **second-dot1q** [*inner-id*| **any**]] [**detail**]]

Use this command to show the statistics for all the 802.1Q VLAN IDs. In the following example, only the outer VLAN ID is displayed:

Note The **any** keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces.

Example:

```
Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

Configuration Examples for PPPoE QinQ Support

Configuring the any Keyword on Subinterfaces for PPPoE QinQ Support Example

Some ambiguous subinterfaces can use the **any** keyword for the inner VLAN ID specification. The **any** keyword represents any inner VLAN ID that is not explicitly configured on any other interface. In the following example, seven subinterfaces are configured with various outer and inner VLAN IDs.

Note The **any** keyword can be configured on only one subinterface of a specified physical interface and outer VLAN ID.

Note The **any** keyword in the **second-dot1q**keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. Therefore, multiple values and ranges for the inner VLAN ID are not supported on IPoQinQ.

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
interface GigabitEthernet1/0/0.3
 encapsulation dot1q 100 second-dot1q 300-400,500-600
interface GigabitEthernet1/0/0.4
 encapsulation dot1q 100 second-dot1q any
interface GigabitEthernet1/0/0.5
 encapsulation dot1q 200 second-dot1q 50
interface GigabitEthernet1/0/0.6
 encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000
```

```
interface GigabitEthernet1/0/0.7
 encapsulation dot1q 200 second-dot1q any
```

The table below shows which subinterfaces are mapped to different values of the outer and inner VLAN IDs on QinQ frames that come in on Gigabit Ethernet (GE) interface 1/0/0.

Table 8 Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0

Outer VLAN ID	Inner VLAN ID	Subinterface Mapped to
100	1 through 99	GigabitEthernet1/0/0.4
100	100	GigabitEthernet1/0/0.1
100	101 through 199	GigabitEthernet1/0/0.4
100	200	GigabitEthernet1/0/0.2
100	201 through 299	GigabitEthernet1/0/0.4
100	300 through 400	GigabitEthernet1/0/0.3
100	401 through 499	GigabitEthernet1/0/0.4
100	500 through 600	GigabitEthernet1/0/0.3
100	601 through 4094	GigabitEthernet1/0/0.4
200	1 through 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 through 999	GigabitEthernet1/0/0.7
200	1000 through 2000	GigabitEthernet1/0/0.6
200	2001 through 2999	GigabitEthernet1/0/0.7
200	3000 through 4000	GigabitEthernet1/0/0.6
200	4001 through 4094	GigabitEthernet1/0/0.7

A new subinterface is now configured:

```
interface GigabitEthernet 1/0/0.8
 encapsulation dot1q 200 second-dot1q 200-600,900-999
```

The table below shows the changes made to the table for the outer VLAN ID of 200. Notice that subinterface 1/0/0.7 configured with the **any** keyword now has new inner VLAN ID mappings.

Table 9 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

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
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	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* • Cisco IOS Master Command List, All Releases

Standards

Standards	Title
IEEE 802.1Q	IEEE Standard for Local and Metropolitan Area Networks

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for PPPoE QinQ Support

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

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

Table 10 Feature Information for PPPoE QinQ Support

Feature Name	Releases	Feature Information
IEEE 802.1Q-in-Q VLAN Tag Termination	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers. Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs.

Feature Name	Releases	Feature Information
PPPoE QinQ Support	Cisco IOS XE Release 2.2	This feature was introduced on Cisco ASR 1000 Series Routers. This feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated. The following commands were introduced or modified: **dot1q tunneling ethertype**, **encapsulation dot1q**, **show vlans dot1q**.

PPPoE Session Limiting on Inner QinQ VLAN

The PPPoE Session Limiting on Inner QinQ VLAN feature allows a service provider to limit each customer to one PPP over Ethernet (PPPoE) client in use by providing the ability to limit the number of PPPoE over QinQ (IEEE 802.1Q VLAN tunnel) sessions based on the inner VLAN ID configured under a subinterface. This capability eliminates the need to configure large numbers of subinterfaces.

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 Table at the end of this document.

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

Prerequisites for PPPoE Session Limiting on Inner QinQ VLAN

- PPPoE server functionality must be configured.
- The PPPoE over IEEE 802.1Q VLANs feature must be configured.

Restrictions for PPPoE Session Limiting on Inner QinQ VLAN

- Do not configure the inner VLAN session limit to be greater than the outer session limit.

Information About PPPoE Session Limiting on Inner QinQ VLAN

Benefits of PPPoE Session Limiting on Inner QinQ VLAN

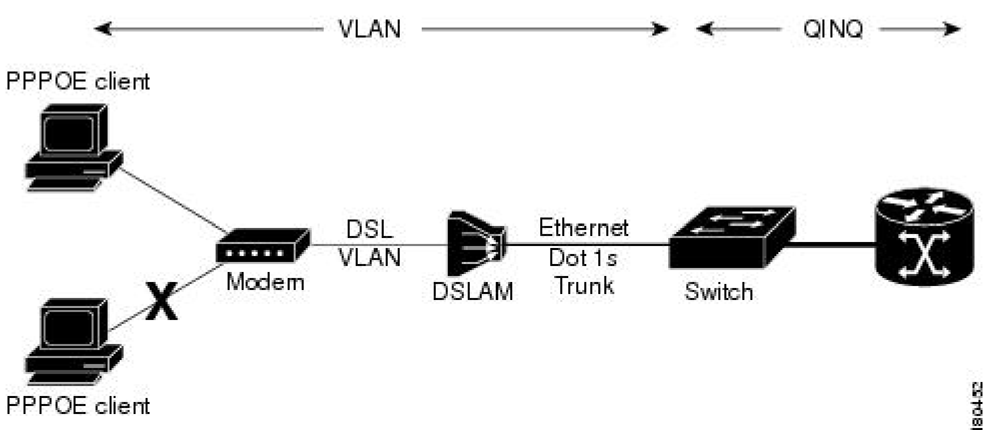
- Facilitates the ability to provision thousands of PPPoE over QinQ sessions having unique inner VLANs using simpler and easier to manage configurations.
- Allows service providers to limit PPPoE sessions based on the QinQ inner VLAN ID.

Feature Design of PPPoE Session Limiting on Inner QinQ VLAN

Prior to the PPPoE Session Limiting on Inner QinQ VLAN feature, PPPoE session limiting required a QinQ subinterface to be configured for each QinQ inner VLAN to be session limited, resulting in configuration requirements that did not scale to large numbers of QinQ VLAN ID pairs. The PPPoE Session Limiting on Inner QinQ VLAN feature adds broadband remote access server (BRAS) capability for configuring a single subinterface for all the unique inner VLAN IDs per outer VLAN while limiting one session per inner VLAN.

The figure below shows a typical implementation of the PPPoE Session Limiting on Inner QinQ VLAN feature.

Figure 6 PPPoE over QinQ Session Limiting



How to Configure PPPoE Session Limiting on Inner QinQ VLAN

Configuring PPPoE Session Limiting on Inner QinQ VLAN

Perform this task to configure PPPoE over QinQ session limiting and allows limiting, which allows you to limit the number of QinQ inner VLAN connections for each customer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **sessions per-vlan limit outer-per-vlan-limit inner inner-per-vlan-limit**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe group 1`	Creates a PPPoE profile and enters the bba-group configuration mode.
Step 4	**sessions per-vlan limit outer-per-vlan-limit inner inner-per-vlan-limit** **Example:** `Router(config-bba-group)#` **sessions per-vlan-limit 400 inner 1**	Configures inner and outer VLAN limits.
Step 5	**end** **Example:** `Router(config-bba-group)#` **end**	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

• Troubleshooting Tips, page 92

Troubleshooting Tips

The following commands can help troubleshoot PPPoE session limiting:

- debug pppoe error
- show pppoe session
- show pppoe summary

Configuration Examples for PPPoE Session Limiting on Inner QinQ VLAN

PPPoE Session Limiting on Inner QinQ VLAN Example

The following example shows how to enable PPPoE over QinQ session limiting on Fast Ethernet interface 1/0/0.1 with outer VLAN ID 10 and a unique inner VLAN ID for each session.

```
Router(config)# bba-group pppoe group1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vlan limit 1000 inner 1
Router(config)#interface eth1/0/0.1
Router(config-subif)# encapsulation dot1q 10 second-dot1q any
Router(config-subif)# enable group group1
```

Additional References

The following sections provide references related to the PPPoE Session Limiting on Inner QinQ VLAN feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
Broadband access commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
IEEE Standard 802.1Q	Virtual Bridged Local Area Networks

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	*PPP over Ethernet*

Technical Assistance

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

Feature Information for PPPoE Session Limiting on Inner QinQ VLAN

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

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

Table 11 Feature Information for PPPoE Session Limiting on Inner QinQ VLAN

Feature Name	Releases	Feature Information
PPPoE Session Limiting on Inner QinQ VLAN	Cisco IOS XE Release 2.1	The PPPoE Session Limiting on Inner QinQ VLAN feature provides the ability to limit the number of PPPoE over QinQ, (IEEE 802.1Q VLAN tunnel) sessions based on the inner VLAN ID configured under a subinterface. In 12.2(31)SB2, this feature was introduced on the Cisco 10000 router. The following command was modified by this feature: **session per-vlan limit**.

PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

The PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature provides a method by which the digital subscriber line access multiplexer (DSLAM) sends the DSL Remote-ID tag in the discovery phase as an identifier for the authentication, authorization, and accounting (AAA) access request on an Fast or Gigabit Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Fast or Gigabit Ethernet instead. This Remote-ID tag is useful for troubleshooting, authentication, and accounting.

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 Table at the end of this document.

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

Prerequisites for 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, page 102 for more information.

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

Differences Between ATM and Fast or Gigabit Ethernet-Based Broadband Access Networks

Broadband DSLAM and Broadband Remote Access Server (BRAS) vendors need to provide Fast or Gigabit Ethernet-based networks as an alternative to an ATM access network, with a DSLAM bridging the ATM-DSL local loop to the Fast or Gigabit Ethernet-based broadband access network and allowing Fast or Gigabit Ethernet-based connectivity to the BRAS. There is no unique mapping between the subscriber Line-ID tag and the interface in an Fast or Gigabit Ethernet broadband access network, as there is in an ATM-based broadband network, where the ATM VC is associated to a subscriber line. During the authentication phase that initiates the PPP access and AAA accounting requests, the BRAS includes a NAS-Port-ID attribute in RADIUS authentication packets that identifies the DSL for the subscriber

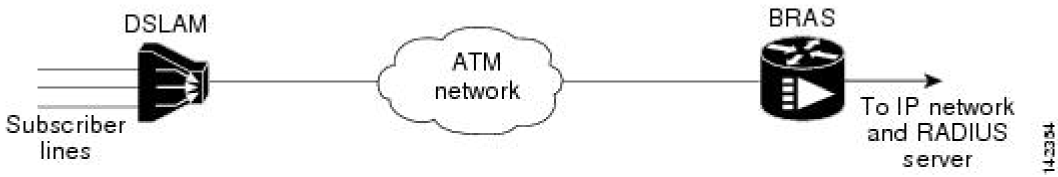
DSL Forum 2004-71 Solution for Remote-ID in PPPoE Discovery Phase

DSL Forum 2004-71 defines a method whereby the DSLAM sends the DSL Remote-ID tag in the PPP over Ethernet (PPPoE) discovery phase to apply the same subscriber mapping capability to Fast or Gigabit Ethernet interfaces that is possible on ATM interfaces. This method adds support for the PPPoE server acting as a BRAS to report the Remote-ID tag as a new vendor specific attribute (VSA) (AAA_AT_REMOTE_ID) in AAA authentication and accounting requests. If the **radius-server attribute 31 remote-id** command is configured on the BRAS, the Remote-ID tag will be sent to a RADIUS server as the Calling Station-ID tag (attribute 31).

Remote-ID Tag in Fast or Gigabit Ethernet-Based Broadband Access Networks

Traditional ATM-based DSL broadband access networks have the topology shown in The figure below.

Figure 7 ***ATM-Based DSL Broadband Access Network***

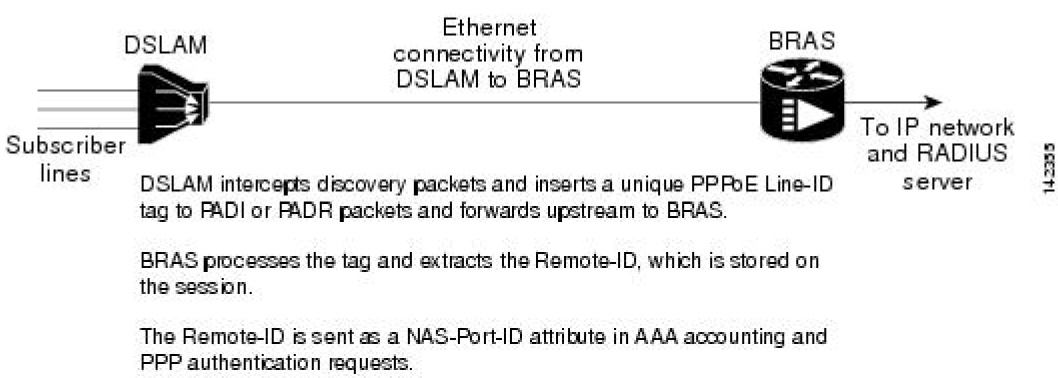


In terms of logical connectivity, there is a one-to-one mapping of the DSL subscriber line to the end user and the ATM virtual circuit (VC) used to carry the PPP session through the DSLAM and to the BRAS, where this VC information is converted into a NAS-Port-ID tag for use in RADIUS packets.

The simple mapping available from an ATM-based broadband network between the physical line in the DSL local loop to the end user and a virtual circuit (from DSLAM to BRAS) is not available for a Fast or Gigabit Ethernet-based network. To solve this problem, the PPPoE Remote-ID Tag Processing feature uses a PPPoE intermediate agent function on the DSLAM to attach a tag to the PPPoE discovery packets. The BRAS then receives the tagged packet, decodes the tag, and inserts the line identifier into RADIUS packets destined for the RADIUS server.

The DSLAM intercepts PPPoE discovery frames from the client or initiates a discovery frame if the PPPoE Active Discovery (PAD) client is a legacy PPP over ATM (PPPoA) device. The DSLAM inserts a unique Remote-ID tag and DSL sync rate tag using the PPPoE vendor-specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) packets; see the figure below. The DSLAM forwards these packets upstream to the BRAS after the insertion. The tag contains the identification of the DSL line on which the PADI or PADR packet was received, in the access node where the intermediate agent resides.

Figure 8 ***PPPoE Remote-ID Tag Processing Solution***



When the **vendor-tag remote-id service** command is configured in broadband access (BBA) group configuration mode, the BRAS processes the received PPPoE vendor-specific tag in the PADR frame and extracts the Remote-ID tag, which is sent to the remote AAA server as a VSA in all AAA access and accounting requests. When the **radius-server attribute 31 remote-id**global configuration command is also configured on the BRAS, the Remote-ID value is inserted into attribute 31.

Outgoing PAD Offer (PADO) and PAD Session-Confirmation (PADS) packets from the BRAS have the DSLAM-inserted Remote-ID tag. The DSLAM should strip the tag out of PADO and PADS frames. If the DSLAM cannot strip off the tag, the BRAS must remove the tag before sending the frames out. This is accomplished using the **vendor-tag strip** BBA group configuration mode command. If this command is configured under the BBA group, the BRAS strips the incoming Remote-ID tag (and any other vendor tag) off of the outgoing PADO and PADS frames. This action complies with DSL Forum Technical Report 101 .

Benefits of the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

The shift toward Fast or Gigabit Ethernet-based DSLAMs offers the following benefits:

- Ability to use simpler and lower-cost provisioning options for DSL subscribers over a Fast or Gigabit Ethernet-based backhaul network rather than on an ATM-based network.
- Ability to use higher bandwidth connectivity options available from Fast or Gigabit Ethernet that are not possible on ATM.
- Ability to upgrade to next-generation DSLAMs with quality of service (QoS), and support for higher bandwidth, asymmetric dual latency modems such as the ADSL2.

Ability to inject high-bandwidth content such as video in a Fast or Gigabit Ethernet network.

How to Configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Configuring the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement Feature

This task describes how to configure the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature. When this feature is configured, BRAS will process the incoming PADR frames and send the Remote-ID field of the incoming tag to the RADIUS server as a VSA.

For DSL-Sync-Rate tags, you must enter the **vendor-tag dsl-sync-rate service** command under a BBA group. When this command is entered, the BRAS will process incoming PADR frames and send the DSL-Sync-Rate tags to the RADIUS server as VSAs.

An Access-Accept message is sent by the RADIUS server and vendor-tag attributes sent in the Access-Request message will be present in the Access-Accept message if the RADIUS server echoes it back.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server attribute 31 remote-id**
5. **bba-group pppoe** *group-name*
6. **vendor-tag remote-id service**
7. **vendor-tag dsl-sync-rate service**
8. **nas-port-id format c**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	(Optional) Enables the AAA access control model.
Step 4	**radius-server attribute 31 remote-id** **Example:** `Router(config)# radius-server attribute 31 remote-id`	(Optional) Sends the Remote-ID tag to the RADIUS server via a new VSA (AAA_AT_REMOTE_ID) and in attribute 31--Calling Station ID.
Step 5	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.

	Command or Action	Purpose
Step 6	**vendor-tag remote-id service** **Example:** `Router(config-bba-group)# vendor-tag remote-id service`	Enables the BRAS to process incoming PADR frames and send the Remote-ID field of the incoming tag to the RADIUS server as a VSA.
Step 7	**vendor-tag dsl-sync-rate service** **Example:** `Router(config-bba-group)# vendor-tag dsl-sync-rate service`	Enables the BRAS to process the incoming PADR frames and send the DSL-Sync-Rate tags to the RADIUS server as VSAs.
Step 8	**nas-port-id format c** **Example:** `Router(config-bba-group)# nas-port-id format c`	Specifies a format for broadband subscriber access line identification coding. • The designation of **format c**is specifically designed for a particular coding format. A sample of this format is as follows: NAS_PORT_ID=atm 31/31/7:255.65535 example001/0/31/63/31/127 • This means the subscriber interface type of the BRAS equipment is an ATM interface. The BRAS slot number is 31, and the BRAS subslot number is 31. The BRAS port number is 7. The virtual path identifier (VPI) is 255, and the virtual circuit identifier (VCI) is 65535. The Circuit-ID/Remote-ID tag is example001/0/31/63/31/127.
Step 9	**end** **Example:** `Router(config-bba-group)#` **end**	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

Stripping Vendor-Specific Tags

Outgoing PADO and PADS packets will have the DSLAM-inserted Remote-ID and DSL-Sync-Rate tags, and the DSLAM must strip these tags from the packets. If the DSLAM cannot strip the tag, the BRAS must remove it before sending out the packets. This task is accomplished through configuration of the **vendor-tag strip** command in BBA group configuration mode. Note that the **vendor-tag strip** command also removes the Circuit-ID tag.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **vendor-tag strip**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile and enters BBA group configuration mode.
Step 4	**vendor-tag strip** **Example:** `Router(config-bba-group)# vendor-tag strip`	Enables the BRAS to strip off incoming vendor-specific tags (including Remote-ID, DSL-Sync-Rate tags, and Circuit-ID) from outgoing PADO and PADS frames.
Step 5	**end** **Example:** `Router(config-bba-group)#` **end**	(Optional) Exits the current configuration mode and enters the privileged EXEC mode.

• Troubleshooting Tips, page 101

Troubleshooting Tips

When you enter the **radius-server attribute 31 remote-id**global configuration command in the PPPoE Agent Remote-ID Tag and DSL Line Characteristics Enhancement feature configuration on the BRAS, you can use the **debug radius** privileged EXEC command to generate a report.

The report includes information about the:

- Incoming access interface
- Location where discovery frames are received
- Details of the sessions being established in PPPoE extended NAS-Port format (format d)

Configuration Examples for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Configuring PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement Example

In the following example, outgoing PADO and PADS packets will retain the incoming Vendor-Specific Circuit-ID tag:

```
Router(config)# radius-server attribute 31 remote-id
!
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag remote-id service
Router(config-bba-group)# vendor-tag dsl-sync-rate service
Router(config-bba-group)# nas-port-id format c
!
Router(config)# interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

Stripping Vendor-Specific Tags Example

In the following example, the BRAS will strip off incoming Vendor-Specific Circuit-ID tags from outgoing PADO and PADS packets:

```
Router(config)# bba-group pppoe rmt-id-tag
Router(config-bba-group)# vendor-tag strip
Router(config)#interface FastEthernet0/0/0.1
Router(config-subif)# encapsulation dot1Q 120
Router(config-subif)# pppoe enable group rmt-id-tag
```

Additional References

The following sections provide references related to the PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature.

Related Documents

Related Topic	Document Title
Configuring Broadband and DSL	*Cisco IOS XE Broadband and DSL Configuration Guide*
RADIUS attributes	RADIUS Attributes Overview and RADIUS IETF Attributes module
DSL Line-ID tag solution	RFC 4679 - DSL Forum Vendor Specific RADIUS Attributes
Migration to Fast or Gigabit Ethernet-based DSL aggregation	DSL Forum Technical Report 101

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE)

Technical Assistance

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

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

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

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

Table 12 Feature Information for PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement

Feature Name	Releases	Feature Information
PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement	Cisco IOS XE Release 2.1.	The PPPoE Agent Remote-ID and DSL Line Characteristics Enhancement feature provides a method by which the digital subscriber line access multiplexer (DSLAM) sends the DSL Remote-ID tag in the discovery phase as an identifier for the authentication, authorization, and accounting (AAA) access request on a Fast or Gigabit Ethernet interface, thereby simulating ATM-based broadband access, but using cost-effective Fast or Gigabit Ethernet instead. This Remote-ID tag is useful for troubleshooting, authentication, and accounting. The following commands were introduced or modified: **radius-server attribute**, **bba-group pppoe group-name**, **vendor-tag remote-id service**, **vendor-tag dsl-sync-rate service**, **nas-port-id format c**.

Glossary

AAA --authentication, authorization, and accounting.

ATM --Asynchronous Transfer Mode.

BBA --broadband access.

BRAS --Broadband Remote Access Server.

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

PADO --PPPoE Active Discovery Offer.

PADR --PPPoE Active Discovery Request.

PADS --PPPoE Active Discovery Session-Confirmation.

PPPoE --Point-to-Point Protocol over Ethernet.

RADIUS --Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

VCI --virtual circuit identifier.

VLAN --virtual local-area network.

VPI --virtual path identifier.

VSA --vendor specific attribute. attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

Enabling PPPoE Relay Discovery and Service Selection Functionality

The PPPoE Relay feature enables an L2TP access concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP network server (LNS) or tunnel switch (multihop node). The relay functionality of this feature allows the LNS or tunnel switch to advertise the services it offers to the client, thereby providing end-to-end control of services between the LNS and a PPPoE client.

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 Table at the end of this document.

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

Prerequisites for 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 Prerequisites for Enabling PPPoE Relay Discovery and Service Selection Functionality, page 107 for more information about these features.

Information About Enabling PPPoE Relay Discovery and Service Selection Functionality

L2TP Active Discovery Relay for PPPoE

The PPPoE protocol described in RFC 2516 defines a method for active discovery and service selection of devices in the network by an LAC. A PPPoE client uses these methods to discover an access concentrator in the network, and the access concentrator uses these methods to advertise the services it offers.

The PPPoE Relay feature allows the active discovery and service selection functionality to be offered by the LNS, rather than just by the LAC. The PPPoE Relay feature implements the Network Working Group Internet-Draft titled *L2TP Active Discovery Relay for PPPoE* . The Internet-Draft describes how to relay PPPoE Active Discovery (PAD) and Service Relay Request (SRRQ) messages over an L2TP control channel (the tunnel). (See the L2TP Active Discovery Relay for PPPoE, page 108 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

Configuring the LAC and Tunnel Switch for PPPoE Relay

Perform this task to configure the LAC and tunnel switch for PPPoE Relay, which configures a subscriber profile that directs PAD messages to be relayed on an L2TP tunnel. The subscriber profile also will contain an authorization key for the outgoing L2TP tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service relay pppoe vpdn group** *vpdn-group-name*
5. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber profile** *profile-name* **Example:** `Router(config)# subscriber profile profile-1`	Configures the subscriber profile name and enters subscriber profile configuration mode. • *profile-name* --Is referenced from a PPPoE profile configured by the **bba-group pppoe** global configuration command, so that all the PPPoE sessions using the PPPoE profile defined by the **bba-group pppoe**command will be treated according to the defined subscriber profile.
Step 4	**service relay pppoe vpdn group** *vpdn-group-name* **Example:** `Router(config-sss-profile)# service relay pppoe vpdn group Group-A`	Provides PPPoE relay service using a VPDN L2TP tunnel for the relay. The VPDN group name specified is used to obtain outgoing L2TP tunnel information. • See the What to Do Next, page 109 section for the equivalent RADIUS profile entry.
Step 5	exit **Example:** `Router(config-sss-profile)# exit`	(Optional) Ends the configuration session and returns to privileged EXEC mode.

• What to Do Next, page 109

What to Do Next

Configure the LNS side of the configuration by performing the tasks described in the next section.

Configuring the LNS (or Multihop Node) to Respond to Relayed PAD Messages

On the router that responds to relayed PAD messages, perform this task to configure a PPPoE group and attach it to a VPDN group that accepts dial-in calls for L2TP. The relayed PAD messages will be passed from the VPDN L2TP tunnel and session to the PPPoE broadband group for receiving the PAD responses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *vpdn-group-name*
4. **accept-dialin**
5. **protocol l2tp**
6. **virtual-template** *template-number*
7. **exit**
8. **terminate-from hostname** *host-name*
9. **relay pppoe bba-group** *pppoe-bba-group-name*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *vpdn-group-name* **Example:** `Router(config)# vpdn-group Group-A`	Creates a VPDN group and enters VPDN group configuration mode.

	Command or Action	Purpose
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from an LAC and creates an accept-dialin VPDN subgroup.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP tunneling protocol.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-vpdn-req-in)# virtual-template 2`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 7	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.
Step 8	**terminate-from hostname** *host-name* **Example:** `Router(config-vpdn)# terminate-from hostname LAC-1`	Specifies the LAC hostname that will be required when the VPDN tunnel is accepted.
Step 9	**relay pppoe bba-group** *pppoe-bba-group-name* **Example:** `Router(config-vpdn)# relay pppoe bba-group group-2`	Specifies the PPPoE BBA group that will respond to the PAD messages. • The PPPoE BBA group name is defined with the **bba-group pppoe** *group-name* global configuration command. • See the Configuring the LNS (or Multihop Node) to Respond to Relayed PAD Messages, page 110 section for the equivalent RADIUS profile entry.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits to global configuration mode.

Monitoring PPPoE Relay

Perform this task to monitor PPPoE Relay.

SUMMARY STEPS

1. **enable**
2. **show pppoe session**
3. **show pppoe relay context all**
4. **clear pppoe relay context**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pppoe session**

Displays information about currently active PPPoE sessions.

Example:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st
     26     19  0001.96da.a2c0  Et0/0.1                  5  N/A RELFWD
                000c.8670.1006  VLAN:3434
```

Step 3 **show pppoe relay context all**

Displays the PPPoE relay context created for relaying PAD messages.

Example:

```
Router# show pppoe relay context all
Total PPPoE relay contexts 1
UID    ID     Subscriber-profile      State
25     18     cisco.com                 RELAYED
```

Example:

Step 4 **clear pppoe relay context**

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

Example:

```
Router(config)# clear pppoe relay context
```


Troubleshooting Tips

Use the following commands in privileged EXEC mode to help you troubleshoot the PPPoE Relay feature:

- **debug ppp forwarding**
- **debug ppp negotiation**
- **debug pppoe events**
- **debug pppoe packets**
- **debug vpdn l2x-events**
- **debug vpdn l2x-packets**

Configuration Examples for Enabling PPPoE Relay Discovery and Service Selection Functionality

PPPoE Relay on LAC Configuration Example

The following is an example of a standard LAC configuration with the commands to enable PPPoE relay added:

```
hostname User2
!
username User1 password 0 field
username User2 password 0 field
username user-group password 0 field
username User5 password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
username User3-lns-domain password 0 field
!
ip domain-name cisco.com
!
vpdn enable
vpdn source-ip 10.0.195.151
!
vpdn-group User2-vpdn-group-domain
 request-dialin
```

```
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.133
 local name User2-lac-domain
!
!
interface Loopback123
 ip address 10.22.2.2 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.195.151 255.255.255.0
 no keepalive
 half-duplex
 pppoe enable group group-1
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback123
 ppp authentication chap
 ppp chap hostname User2-lac-domain
!
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
subscriber profile Profile1
 service relay pppoe vpdn group User2-vpdn-group-domain
!
bba-group pppoe group-1
 virtual-template 1
 service profile Profile1
!
```

Basic LNS Configured for PPPoE Relay Example

The following example shows the basic configuration for an LNS with commands added for PPPoE relay:

```
hostname User5
!
!
username User5 password 0 field
username user-group password 0 field
username User1 password 0 field
username User2 password 0 field
username User3 password 0 field
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 field
username mysgbpgroup password 0 cisco
username User3-lns-domain password 0 field
username User2-lac-domain password 0 field
username User1-client-domain@cisco.net password 0 field
username User5-mh password 0 field
username User1@domain.net password 0 field
ip subnet-zero
!
!
ip domain-name cisco.com
!
vpdn enable
vpdn multihop
vpdn source-ip 10.0.195.133
!
vpdn-group 1
 request-dialin
  protocol l2tp
!
vpdn-group 2
! Default L2TP VPDN group
 accept-dialin
```

```
  protocol l2tp
!
vpdn-group User5-mh
 request-dialin
  protocol l2tp
  domain cisco.net
 initiate-to ip 10.0.195.143
 local name User5-mh
!
vpdn-group User3-vpdn-group-domain
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname User2-lac-domain
 local name User3-lns-domain
 relay pppoe group group-1
!
!
interface Loopback0
 no ip address
!
!
interface Loopback123
 ip address 10.23.3.2 255.255.255.0
!
!
interface FastEthernet0/0
 ip address 10.0.195.133 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
!
!
interface Virtual-Template2
 mtu 1492
 ip unnumbered Loopback123
 ip access-group virtual-access3#234 in
 ppp mtu adaptive
 ppp authentication chap
 ppp chap hostname User3-lns-domain
!
!
ip default-gateway 10.0.195.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
bba-group pppoe group-1
 virtual-template 2
!
```

Tunnel Switch (or Multihop Node) Configured to Respond to PAD Messages Example

The following is an example of a standard tunnel switch configuration with the commands to enable response to PPPoE relay messages added:

```
hostname User3
!
!
username User1 password 0 room1
username User2 password 0 room1
username User3 password 0 room1
username User1@domain.net password 0 room1
username User3-lns-dnis password 0 cisco
username User3-lns-domain password 0 room1
username User2-lac-dnis password 0 cisco
username User2-lac-domain password 0 room1
username User5 password 0 room1
```

```
username User5-mh password 0 room1
username user-group password 0 room1
username User3-dialout password 0 cisco
username User2-dialout password 0 cisco
username abc password 0 cisco
username dial-7206a password 0 room1
username mysgbpgroup password 0 cisco
username User1-client-domain@cisco.net password 0 room1
username User4-lns-domain password 0 room1
!
ip domain-name cisco.com
!
vpdn enable
!
vpdn-group User3-mh
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname User5-mh
 relay pppoe bba-group group-1
!
interface Loopback0
 ip address 10.4.4.2 255.255.255.0
!
interface Loopback1
 ip address 10.3.2.2 255.255.255.0
!
interface Ethernet2/0
 ip address 10.0.195.143 255.255.0.0
 half-duplex
 no cdp enable
!
interface Virtual-Template1
 mtu 1492
 ip unnumbered Loopback0
 no keepalive
 ppp mtu adaptive
 ppp authentication chap
 ppp chap hostname User3-lns-domain
!
ip default-gateway 10.0.195.1
ip route 0.0.0.0 0.0.0.0 10.0.195.1
!
!
bba-group pppoe group-1
 virtual-template 1
!
```

Tunnel Switch Configured to Relay PAD Messages Example

The following partial example shows a configuration that allows the tunnel switch to relay PAD messages:

```
subscriber profile profile-1
! Configure profile for PPPoE Relay
 service relay pppoe vpdn group Example1.net
.
.
.
vpdn-group Example2.net
! Configure L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from host Host1
 relay pppoe bba-group group-1
.
.
.
vpdn-group Example1.net
```

```
! Configure L2TP tunnel for PPPoE Relay
 request-dialin
  protocol l2tp
.
.
.
 initiate-to ip 10.17.1.3
.
.
.
! PPPoE-group configured for relay
bba-group pppoe group-1
.
.
.
service profile profile-1
```

RADIUS Subscriber Profile Entry for the LAC Example

The following example shows how to enter Subscriber Service Switch subscriber service attributes in a AAA RADIUS server profile.

```
profile-1 = profile-name.
.
.
```

Cisco:Cisco-Avpair = "sss:sss-service=relay-pppoe"

The following is an example of a typical RADIUS subscriber profile entry for an LAC:

```
cisco.com Password = "password"
    Cisco:Cisco-Avpair = "sss:sss-service=relay-pppoe",
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Tunnel-Assignment-Id = assignment-id
```

RADIUS VPDN Group User Profile Entry for the LNS Example

The following example shows how to enter the VPDN group attributes in a AAA RADIUS server profile.

```
profile-1 = profile-name.
.
.
   Cisco:Cisco-Avpair = "vpdn:relay-pppoe-bba-group=group-name
```

The following is an example of a typical RADIUS subscriber profile entry for an LNS:

```
cisco.com Password = "password"
    Tunnel-Type = L2TP,
    Tunnel-Server-Endpoint = .....,
    Tunnel-Client-Auth-ID = "client-id",
    Tunnel-Server-Auth-ID = "server-id",
    Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=password",
    Cisco:Cisco-Avpair = "vpdn:l2tp-nosession-timeout=never",
    Cisco:Cisco-Avpair = "vpdn:relay-pppoe-bba-group=group-name"
    Tunnel-Assignment-Id = assignment-id
```

Additional References

The following sections provide referenced related to the PPPoE Relay feature.

Related Documents

Related Topic	Document Title
VPDN tunnels	*Cisco IOS XE Dial Technologies Configuration Guide*
VPDN tunnel commands	*Cisco IOS XE Dial Technologies Configuration Guide*
Tunnel switching	L2TP Tunnel Switching feature module
PPPoE broadband groups	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
PPPoE broadband commands	*Cisco IOS XE Broadband Access Aggregation and DSL Command Reference*
Broadband access aggregation concepts	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*
Tasks for preparing for broadband access aggregation	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
RFC 2516	*Method for Transmitting PPP Over Ethernet (PPPoE)*

RFCs	Title
RFC 3817	• *L2TP Active Discovery Relay for PPPoE* • Network Working Group Internet-Draft, *L2TP Active Discovery Relay for PPPoE* , which can be seen at http://tools.ietf.org/html/draft-dasilva-l2tp-relaysvc-06

Technical Assistance

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

Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

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

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

Table 13 Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

Feature Name	Releases	Feature Configuration Information
PPPoE Relay	Cisco IOS XE Release 2.1	The PPPoE Relay feature enables an L2TP access concentrator (LAC) to relay active discovery and service selection functionality for PPP over Ethernet (PPPoE), over a Layer 2 Tunneling Protocol (L2TP) control channel, to an L2TP network server (LNS) or tunnel switch (multihop node). This feature was integrated into Cisco IOS XE Release 2.1.
PPPoE Service Selection	Cisco IOS XE Release 2.4	This feature was integrated into Cisco IOS XE Release 2.4.

Configuring Cisco Subscriber Service Switch Policies

The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. The primary focus of the Subscriber Service Switch is to direct PPP from one point to another using a Layer 2 subscriber policy. The policy manages tunneling of PPP in a policy-based bridging fashion.

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 Table at the end of this document.

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

Prerequisites for Configuring a Subscriber Service Switch Policy

- Before configuring a Subscriber Service Switch policy, you must understand the concepts presented in the "Understanding Broadband Access Aggregation" module.
- Before configuring a Subscriber Service Switch policy, you must perform the PPP over Ethernet (PPPoE) configuration procedures in the "Providing Protocol Support for Broadband Access

Aggregation of PPPoE Sessions" module or perform the PPP over ATM (PPPoA) configuration procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions" module.

Restrictions for Configuring a Subscriber Service Switch Policy

The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. The Subscriber Server Switch provides the infrastructure for any protocol to plug into; however, the initial implementation provides switching PPP over Ethernet and PPP over ATM session to a Layer 2 Tunneling Protocol (L2TP) device such as an L2TP access concentrator (LAC) switch, and switching L2TP sessions to an L2TP tunnel switch only.

Information About the Subscriber Service Switch

The Subscriber Service Switch was developed in response to a need by Internet service providers (ISPs) for increased scalability and extensibility for remote access service selection and Layer 2 subscriber policy management. This Layer 2 subscriber policy is needed to manage tunneling of PPP in a policy-based bridging fashion.

- Benefits of the Subscriber Service Switch, page 122
- Backward Compatibility of Subscriber Service Switch Policies, page 123
- Debug Commands Available for Subscriber Service Switch, page 125

Benefits of the Subscriber Service Switch

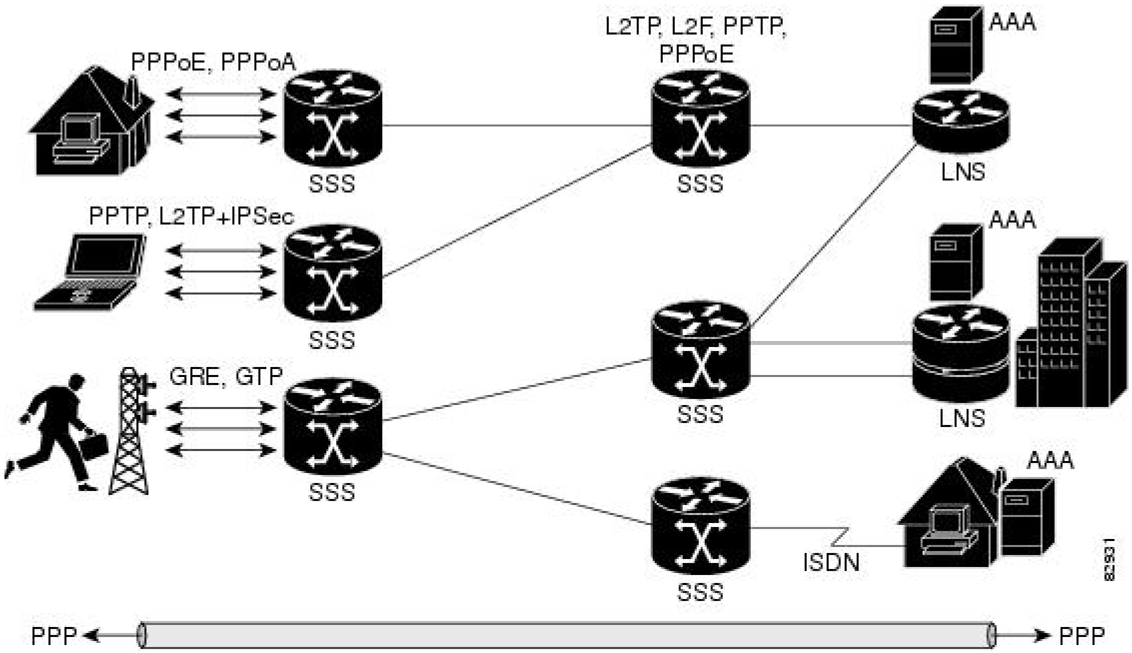
The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. In the past, remote access service selection was largely determined by the telephone number dialed or the PPP username and password entered during a PPP authentication cycle. However, broadband, cable, Virtual Private Network (VPN), and wireless access methods have created an environment where PPP sessions may be tunneled over a variety of protocols and media. The multitude of protocols, management domains, network infrastructure, and variety of services has created a complex environment for directing a subscriber to a given service or application. The problem is further complicated by the much greater density of total PPP sessions that can be transported over shared media versus traditional point-to-point links. The Subscriber Service Switch can provide a flexible and extensible decision point linking an incoming subscriber (typically a PPP session over some physical or virtual link) to another tunneled link or local termination for Layer 3 processing.

The Subscriber Service Switch is also scalable in situations where a subscriber's Layer 2 service is switched across virtual links. Examples include switching among PPPoA, PPPoE, L2TP, Layer 2 Forwarding Protocol (L2F), Point-to-Point Tunneling Protocol (PPTP), generic routing encapsulation (GRE), and General Packet Radio Service (GPRS) Tunneling Protocol (GTP wireless data standard).

The figure below shows how the Subscriber Service Switch provides its own centralized switching path that bypasses the virtual-access-based switching available earlier. In the figure below, the Subscriber

Service Switch is switching data traffic from personal computers in a home and corporate office and from a wireless user.

Figure 9 ***Basic Subscriber Service Switch Operation***



Protocols that register with the Subscriber Service Switch application programming interface (API) can take advantage of this switching path. Bypassing the virtual access interface in this manner helps the Cisco IOS XE software to scale to the increased number of sessions that the market demands. The Subscriber Service Switch also improves network performance. For example, benchmark testing indicates that performance of L2TP multihop tasks occurs twice as fast in networks with the Subscriber Service Switch as in networks without it.

Backward Compatibility of Subscriber Service Switch Policies

All of the existing virtual private dialup network (VPDN), Multichassis Multilink PPP (MMLP), and local termination policies and configurations are maintained in the implementation of the Subscriber Service Switch; however, default policies may be overridden by the following configurations or events:

- Resource Manager (RM) VPDN authorization is attempted before VPDN authorization.
- VPDN authorization is attempted before Stack Group Forwarding (SGF) MMLP.
- VPDN service authorization is attempted only when the **vpdn enable** command is configured.
- RM VPDN service authorization is attempted only if RM is enabled.
- SGF authorization is attempted only when the **sgbp member** command is configured and one or both of the following service keys are available from the subscriber: unauthenticated PPP name and endpoint discriminator.
- The **dnis** and **domain** service keys, in that order, are used to authorize VPDN service, provided that VPDN service is enabled.
- An unauthenticated PPP name is always reduced to a domain name by taking all characters from the right of the PPP name up to a configurable delimiter character (default is the @ character). Only the domain portion is used to locate a service.

- If the **vpdn authen-before-forward** command is configured as a global configuration command, the authenticated PPP name is used to authorize VPDN service.
- The **vpdn-group** command can define four configurations:
- Authorization for VPDN call termination (using the *accept-dialin* and **accept-dialout** keywords).
- Authorization for VPDN subscriber service (using the **request-dialin** and **request-dialout** keywords).
- A directive to collect further service keys and reauthorize (using the **authen-before-forward** keyword).
- A tunnel configuration.

The Subscriber Service Switch adds a general configuration framework to replace the first three aspects of a VPDN group.

- If VPDN and SGF services either are not configured or cannot be authorized, local PPP termination service is selected. Further PPP authorization is still required to complete local termination.
- A two-phase authorization scheme is enabled by the **vpn domain authorization** command. An NAS-Port-ID (NAS port identifier) key is used to locate the first service record, which contains a restricted set of values for the domain substring of the unauthenticated PPP name. This filtered service key then locates the final service. Cisco refers to this scheme as domain preauthorization.
- Domain preauthorization will occur only when the **NAS-Port-ID** key is available.
- When domain preauthorization is enabled, both authenticated and unauthenticated domain names are checked for restrictions.
- It is possible to associate a fixed service with an ATM permanent virtual circuit (PVC), thus affecting any subscribers carried by the PVC. The **vpn service** command, in ATM VC or VC class configuration mode, and the associated key make up the generic service key.
- When the generic service key is available, it will be used for authorization instead of the unauthenticated domain name.
- If either the **vpdn authen-before-forward** or **per vpdn-group authen-before-forward** command is configured, the authenticated username is required and will be used to authorize VPDN service.
- To determine whether the **authen-before-forward** command is configured in a VPDN group (using the **vpdn-group** command), an unauthenticated username or the generic service key is required as the initial-want key set.
- When the global **vpdn authen-before-forward** command is not configured, the generic service key, if one is available, is used to determine whether the **authen-before-forward** function is configured in the VPDN group (using the **vpdn-group** command). If the generic service key is not available, the unauthenticated username will be used.
- If an accounting-enabled key is available, the unauthenticated username is required.
- VPDN multihop is allowed only when VPDN multihop is enabled.
- SGF on the L2TP network server (LNS) is allowed only when VPDN multihop is enabled on the LNS.
- Forwarding of SGF calls on the LAC is allowed only if VPDN multihop is enabled on the LAC.
- SGF-to-SGF multihop is not allowed.
- When PPP forwarding is configured, both Multilink PPP (MLP) and non-MLP calls are forwarded to the winner of the Stack Group Bidding Protocol (SGBP) bid.
- Authentication is always required for forwarded Packet Data Serving Node (PDSN) calls.
- When the **directed-request** function is enabled and activated using the **ip host** command, VPDN service authorization occurs only when the **vpdn authorize directed-request** command is used.
- Fixed legacy policy is still maintained for RM.

Debug Commands Available for Subscriber Service Switch

The Subscriber Service Switch feature introduces five new EXEC mode **debug** commands to enable diagnostic output about Subscriber Service Switch call operation, as follows:

- **debug sss aaa authorization event** --Displays messages about AAA authorization events that are part of normal call establishment.
- **debug sss aaa authorization fsm** --Displays messages about AAA authorization state changes.
- **debug sss error** --Displays diagnostic information about errors that may occur during Subscriber Service Switch call setup.
- **debug sss event** --Displays diagnostic information about Subscriber Service Switch call setup events.
- **debug sss fsm** --Displays diagnostic information about the Subscriber Service Switch call setup state.

The following EXEC mode debug commands already exist:

- **debug redundancy** - This command is available on platforms that support redundancy.
- **debug sss elog** --Collects SSS performance event data.
- **debug sss feature** --Enables debug for SSS feature events
- **debug sss packet** --Enables packet level event and information debugging for the Subscriber Service Switch.
- **debug sss policy** --Enables debug for SSS policy module events.
- **debug sss service** --Enables debug for service manager event.

These commands were designed to be used with Cisco IOS XE **debug** commands that exist for troubleshooting PPP and other Layer 2 call operations. The table below lists some of these **debug** commands.

Table 14 Additional Debugging Commands for Troubleshooting the Subscriber Service Switch

Command	Purpose
debug ppp negotiation	Allows you to check that a client is passing PPP negotiation information.
debug pppoe errors	Displays PPPoE error messages.
debug pppoe events	Displays protocol event information.
debug vpdn call events	Enables VPDN call event debugging.
debug vpdn call fsm	Enables VPDN call setup state debugging.
debug vpdn elog	Enables VPDN performance event data collection.
debug vpdn events	Displays PPTP tunnel event change information.
debug vpdn 12x-data	Enables L2F and L2TP event and data debugging.
debug vpdn l2x-errors	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.

Command	Purpose
debug vpdn l2x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn 12x-packets	Enables L2F and L2TP packet level debugging.
debug vpdn errors	Displays PPTP protocol error messages.
debug vpdn message	Enables VPDN inter processing message debugging.
debug vpdn packet	Enables VPDN packet level debugging.
debug vpdn scalability	Enables VPDN scalability debugging.
debug vpdn sss errors	Displays diagnostic information about errors that may occur during VPDN Subscriber Service Switch call setup.
debug vpdn sss events	Displays diagnostic information about VPDN Subscriber Service Switch call setup events.

Note The **debug** commands are intended only for troubleshooting purposes, because the volume of output generated by the software can result in severe performance degradation on the router.

How to Configure a Subscriber Service Switch Policy

The Subscriber Service Switch architecture is transparent, and existing PPP, VPDN, PPPoE, PPPoA, and authentication, authorization, and accounting (AAA) call configurations will continue to work in this environment. You can, however, enable Subscriber Service Switch preauthorization and Subscriber Service Switch type authorization. You may also find it helpful to verify Subscriber Service Switch call operation.

- Enabling Domain Preauthorization on a NAS, page 126
- Creating a RADIUS User Profile for Domain Preauthorization, page 127
- Enabling a Subscriber Service Switch Preauthorization, page 128
- Troubleshooting the Subscriber Service Switch, page 129

Enabling Domain Preauthorization on a NAS

Perform the following task to enable the NAS to perform domain authorization before tunneling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. vpdn authorize domain
4. **exit**
5. Router# show running-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	vpdn authorize domain **Example:** `Router(config)# vpdn authorize domain`	Enables domain preauthorization on an Network Access Server (NAS).
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 5	Router# show running-config **Example:** `show running-config`	Displays the configuration so you can check that you successfully enabled domain preauthorization.

• What to Do Next, page 127

What to Do Next

Create a RADIUS user profile for domain preauthorization. See the next section for more information.

Creating a RADIUS User Profile for Domain Preauthorization

The table below contains the attributes needed to enable domain preauthorization in a RADIUS user file. Refer to the Cisco IOS XE Security Configuration Guide for information about creating a RADIUS user profile.

Table 15 Attributes for the RADIUS User Profile for Domain Preauthorization

RADIUS Entry	Purpose
nas-port: *ip-address:slot/subslot/port/vpi.vci*	Configures the NAS port username for domain preauthorization. • *ip-address* **:** --Management IP address of the node switch processor (NSP). • *slot* / *subslot* / *port* --Specifies the ATM interface. • *vpi* **.** *vci* --Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.
Password= "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service type as outbound.
Cisco-AVpair= "vpdn:vpn-domain-list= *domain1*, domain2,..."	Specifies the domains accessible to the user. • *domain* --Domain to configure as accessible to the user.

Enabling a Subscriber Service Switch Preauthorization

When Subscriber Service Switch preauthorization is enabled on an LAC, local configurations for session limit per VC and per VLAN are overwritten by the per-NAS-port session limit downloaded from the server. Perform this task to enable preauthorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id**[*aaa-method-list*]
4. **show sss session [all]**
5. exit

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**subscriber access** {**pppoe** | **pppoa**} **pre-authorize nas-port-id**[*aaa-method-list*] **Example:** **Example:** `Router(config)# subscriber access pppoe pre-authorize nas-port-id mlist-llid` **Example:**	Enables Subscriber Service Switch preauthorization. **Note** The LACs maintain a current session number per NAS port. As a new session request comes in, the LAC makes a preauthorization request to AAA to get the session limit, and compares it with the number of sessions currently on that NAS port. This command ensures that session limit querying is only enabled for PPPoE-type calls, not for any other call types.
Step 4	**show sss session [all]** **Example:** `Router(config)# show sss session all`	Displays the Subscriber Service Switch session status.
Step 5	exit **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode.

- What to Do Next, page 129

What to Do Next

Information about troubleshooting a network running the Subscriber Service Switch can be found in the next section.

Troubleshooting the Subscriber Service Switch

Perform this task to troubleshoot the Subscriber Service Switch. Examples of normal and failure operations can be found in the Troubleshooting the Subscriber Service Switch Examples, page 134. Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Perform the following task to troubleshoot a network running the Subscriber Service Switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Use Telnet to access a router port and repeat Steps 2 and 3.
5. **terminal monitor**
6. **exit**
7. **debug sss** *command-option*
8. **configure terminal**
9. **no terminal monitor**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no logging console** **Example:** `Router(config)# no logging console`	Disables all logging to the console terminal. • To reenable logging to the console, use the **logging console** command.
Step 4	Use Telnet to access a router port and repeat Steps 2 and 3.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 5	**terminal monitor** **Example:** `Router(config)# terminal monitor`	Enables logging output on the virtual terminal.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.
Step 7	**debug sss** *command-option* **Example:** `Router# debug sss error`	Enables the **debug** command. **Note** You can enter more than one **debug** command.
Step 8	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 9	**no terminal monitor** **Example:** `Router(config)# no terminal monitor`	Disables logging on the virtual terminal.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Configuration Examples for Configuring a Subscriber Service Switch Policy

LAC Domain Authorization Example

The following example shows the configuration necessary for the LAC to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Domain Preauthorization RADIUS User Profile Example

The following example shows a typical domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
 check_items= {
 2=cisco
 }
 reply_attributes= {
 9,1="vpdn:vpn-domain-list=example1.com,example2.com"
 6=5
 }
 }
 }
```

Subscriber Service Switch Preauthorization Example

The following partial example signals the Subscriber Service Switch to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to all sessions with a PPPoE access type.

```
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist-llid
!
```

Verify Subscriber Service Switch Call Operation Example

The following example command output from the **show sss session all** command provides an extensive report of Subscriber Service Switch session activity. Each section shows the unique identifier for each session, which can be used to correlate that particular session with the session information retrieved from other **show** commands or **debug** command traces. See the following **show vpdn session** command output for an example of this unique ID correlation.

```
Router# show sss session all
```

```
Current SSS Information: Total sessions 9
SSS session handle is 40000013, state is connected, service is VPDN
Unique ID is 9
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:49
Root SIP Handle is DF000010, PID is 49
AAA unique ID is 10
Current SIP options are Req Fwding/Req Fwde
SSS session handle is B0000017, state is connected, service is VPDN
Unique ID is 10
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:05
Root SIP Handle is B9000015, PID is 49
AAA unique ID is 11
Current SIP options are Req Fwding/Req Fwded
SSS session handle is D6000019, state is connected, service is VPDN
Unique ID is 11
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:13
Root SIP Handle is D0000016, PID is 49
AAA unique ID is 12
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 8C000003, state is connected, service is VPDN
Unique ID is 3
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user3@example.com
Last Changed 2d21h
Root SIP Handle is D3000002, PID is 49
AAA unique ID is 3
Current SIP options are Req Fwding/Req Fwded
SSS session handle is BE00000B, state is connected, service is Local Term
Unique ID is 6
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user1
Last Changed 00:03:56
Root SIP Handle is A9000009, PID is 49
AAA unique ID is 7
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DC00000D, state is connected, service is Local Term
Unique ID is 7
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user2
Last Changed 00:03:57
Root SIP Handle is 2C00000A, PID is 49
AAA unique ID is 8
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DB000011, state is connected, service is VPDN
Unique ID is 8
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@example.com
Last Changed 00:02:58
Root SIP Handle is 1000000F, PID is 49
AAA unique ID is 9
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 3F000007, state is connected, service is Local Term
Unique ID is 2
SIP subscriber access type(s) are PPP
Identifier is user1
Last Changed 00:05:30
Root SIP Handle is 8A000009, PID is 92
AAA unique ID is 1
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 97000005, state is connected, service is VPDN
Unique ID is 4
SIP subscriber access type(s) are PPP
Identifier is nobody2@example.com
Last Changed 00:07:16
Root SIP Handle is 32000000, PID is 92
AAA unique ID is 5
Current SIP options are Req Fwding/Req Fwded
```

Correlating the Unique ID in show vpdn session Command Output

The following partial sample output from the **show vpdn session** command provides extensive reports on call activity for all L2TP, L2F, and PPPoE sessions, and identifies the unique ID for each session.

```
Router# show vpdn session all
L2TP Session Information Total tunnels 1 sessions 4
Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody3@example.com
    Interface
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8
Session id 6 is up, tunnel id 13695
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody3@example.com
    Interface
    Remote session id is 693, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 9
```

Troubleshooting the Subscriber Service Switch Examples

This section provides the following debugging session examples for a network running the Subscriber Service Switch:

Reports from **debug** commands should be sent to technical personnel at Cisco Systems for evaluation.

Troubleshooting the Subscriber Service Switch Operation Example

The following example shows the **debug** commands used and sample output for debugging Subscriber Service Switch operation:

```
Router# debug sss event
Router# debug sss error
Router# debug sss state
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on
*Mar  4 21:33:18.248: SSS INFO: Element type is Access-Type, long value is 3
*Mar  4 21:33:18.248: SSS INFO: Element type is Switch-Id, long value is -1509949436
*Mar  4 21:33:18.248: SSS INFO: Element type is Nasport, ptr value is 6396882C
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:18.248: SSS INFO: Element type is AAA-ACCT_ENBL, long value is 1
*Mar  4 21:33:18.248: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:18.248: SSS PM [uid:7]: Need the following key: Unauth-User
*Mar  4 21:33:18.248: SSS PM [uid:7]: Received Service Request
*Mar  4 21:33:18.248: SSS PM [uid:7]: Event <need keys>, State: initial-req to
need-init-keys
*Mar  4 21:33:18.248: SSS PM [uid:7]: Policy reply - Need more keys
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Got reply Need-More-Keys from PM
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Event policy-or-mgr-more-keys, state changed from
wait-for-auth to wait-for-req
*Mar  4 21:33:18.248: SSS MGR [uid:7]: Handling More-Keys event
*Mar  4 21:33:20.256: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Mar  4 21:33:20.256: SSS INFO: Element type is AccIe-Hdl, ptr value is 78000006
*Mar  4 21:33:20.256: SSS INFO: Element type is AAA-Id, long value is 7
*Mar  4 21:33:20.256: SSS INFO: Element type is Access-Type, long value is 0
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Event service-request, state changed from
wait-for-req to wait-for-auth
*Mar  4 21:33:20.256: SSS MGR [uid:7]: Handling Policy Authorize (1 pending sessions)
*Mar  4 21:33:20.256: SSS PM [uid:7]: Received More Initial Keys
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <rcvd keys>, State: need-init-keys to
check-auth-needed
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling Authorization Check
*Mar  4 21:33:20.256: SSS PM [uid:7]: Event <send auth>, State: check-auth-needed to
authorizing
*Mar  4 21:33:20.256: SSS PM [uid:7]: Handling AAA service Authorization
*Mar  4 21:33:20.256: SSS PM [uid:7]: Sending authorization request for 'example.com'
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Event <make request>, state changed from
idle
to authorizing
*Mar  4 21:33:20.256: SSS AAA AUTHOR [uid:7]:Authorizing key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:AAA request sent for key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Received an AAA pass
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <found service>, state changed from
authorizing to complete
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Found service info for key example.com
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Event <free request>, state changed from
complete to terminal
*Mar  4 21:33:20.260: SSS AAA AUTHOR [uid:7]:Free request
*Mar  4 21:33:20.264: SSS PM [uid:7]: Event <found>, State: authorizing to end
*Mar  4 21:33:20.264: SSS PM [uid:7]: Handling Service Direction
*Mar  4 21:33:20.264: SSS PM [uid:7]: Policy reply - Forwarding
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Got reply Forwarding from PM
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Event policy-start-service-fsp, state changed from
wait-for-auth to wait-for-service
*Mar  4 21:33:20.264: SSS MGR [uid:7]: Handling Connect-Forwarding-Service event
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Event service-fsp-connected, state changed from
```

```
wait-for-service to connected
*Mar  4 21:33:20.272: SSS MGR [uid:7]: Handling Forwarding-Service-Connected event
```

Troubleshooting the Subscriber Service Switch on the LAC--Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LAC:

```
Router# debug sss event
Router# debug sss error
Router# debug sss aaa authorization event
Router# debug sss aaa authorization fsm
Router# debug pppoe events
Router# debug pppoe errors
Router# debug ppp negotiation
Router# debug vpdn l2x-events
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn call events
Router# debug vpdn call fsm
Router# debug vpdn events
Router# debug vpdn errors
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS AAA authorization event debugging is on
  SSS AAA authorization FSM debugging is on
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE protocol errors debugging is on
PPP:
  PPP protocol negotiation debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
  VPDN call event debugging is on
  VPDN call FSM debugging is on
  VPDN events debugging is on
  VPDN errors debugging is on
*Nov 15 12:23:52.523: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:23:52.523: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:23:52.527: PPPoE : encap string prepared
*Nov 15 12:23:52.527: [13]PPPoE 10: Access IE handle allocated
*Nov 15 12:23:52.527: [13]PPPoE 10: pppoe SSS switch updated
*Nov 15 12:23:52.527: [13]PPPoE 10: Service request sent to SSS
*Nov 15 12:23:52.527: [13]PPPoE 10: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:23:52.547: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:23:52.547: SSS INFO: Element type is Switch-Id, long value is 2130706444
*Nov 15 12:23:52.547: SSS INFO: Element type is Nasport, ptr value is 63C07288
*Nov 15 12:23:52.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:52.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:52.547: SSS PM [uid:13]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:23:52.547: SSS PM [uid:13]: Received Service Request
*Nov 15 12:23:52.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy requires 'Unauth-User' key
*Nov 15 12:23:52.547: SSS PM [uid:13]: Policy reply - Need more keys
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Got reply Need-More-Keys from PM
*Nov 15 12:23:52.547: SSS MGR [uid:13]: Handling More-Keys event
*Nov 15 12:23:52.547: [13]PPPoE 10: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:23:52.547: [13]PPPoE 10: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
```

```
*Nov 15 12:23:52.547: ppp13 PPP: Using default call direction
*Nov 15 12:23:52.547: ppp13 PPP: Treating connection as a dedicated line
*Nov 15 12:23:52.547: ppp13 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:23:52.547: ppp13 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:23:52.547: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.547: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:52.547: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:52.547: [13]PPPoE 10: State START_PPP    Event DYN_BIND
*Nov 15 12:23:52.547: [13]PPPoE 10: data path set to PPP
*Nov 15 12:23:52.571: ppp13 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:    MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:52.571: ppp13 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:23:52.571: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:52.571: ppp13 LCP:    MagicNumber 0x0017455D (0x05060017455D)
*Nov 15 12:23:54.543: ppp13 LCP: TIMEout: State ACKsent
*Nov 15 12:23:54.543: ppp13 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:23:54.543: ppp13 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:23:54.543: ppp13 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:23:54.543: ppp13 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
*Nov 15 12:23:54.543: ppp13 LCP: State is Open
*Nov 15 12:23:54.543: ppp13 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:23:54.543: ppp13 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:23:54.547: ppp13 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
*Nov 15 12:23:54.547: ppp13 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:23:54.547: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Nov 15 12:23:54.547: SSS INFO: Element type is AccIe-Hdl, ptr value is B200000C
*Nov 15 12:23:54.547: SSS INFO: Element type is AAA-Id, long value is 14
*Nov 15 12:23:54.547: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:23:54.547: SSS MGR [uid:13]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:23:54.547: SSS PM [uid:13]: Received More Keys
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling Authorization Check
*Nov 15 12:23:54.547: SSS PM [uid:13]: Handling AAA service Authorization
*Nov 15 12:23:54.547: SSS PM [uid:13]: Sending authorization request for 'example.com'
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:Authorizing key example.com
*Nov 15 12:23:54.547: SSS AAA AUTHOR [uid:13]:AAA request sent for key example.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Received an AAA pass
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Found service info for key example.com
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:23:54.551: SSS AAA AUTHOR [uid:13]:Free request
*Nov 15 12:23:54.551: SSS PM [uid:13]: Handling Service Direction
*Nov 15 12:23:54.551: SSS PM [uid:13]: Policy reply - Forwarding
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Got reply Forwarding from PM
*Nov 15 12:23:54.551: SSS MGR [uid:13]: Handling Connect-Service event
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Event connect req, state changed from idle
to connecting
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Requesting connection
*Nov 15 12:23:54.551: VPDN CALL [uid:13]: Call request sent
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Event client connect, state changed from
idle to connecting
*Nov 15 12:23:54.551: VPDN MGR [uid:13]: Initiating compulsory connection to
192.168.8.2
*Nov 15 12:23:54.551:   Tnl/Sn61510/7 L2TP: Session FS enabled
*Nov 15 12:23:54.551:   Tnl/Sn61510/7 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:23:54.551: uid:13  Tnl/Sn61510/7 L2TP: Create session
*Nov 15 12:23:54.551: uid:13  Tnl/Sn61510/7 L2TP: O ICRQ to rp1 9264/0
*Nov 15 12:23:54.551: [13]PPPoE 10: Access IE nas port called
*Nov 15 12:23:54.555:   Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.555: uid:13  Tnl/Sn61510/7 L2TP: Session state change from
wait-for-tunnel to wait-reply
```

```
*Nov 15 12:23:54.555: [13]PPPoE 10: State LCP_NEGO    Event PPP_FWDING
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: O ICCN to rp1 9264/13586
*Nov 15 12:23:54.559:   Tnl61510 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: Session state change from
wait-reply to established
*Nov 15 12:23:54.559: uid:13  Tnl/Sn61510/7 L2TP: VPDN session up
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Event peer connected, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: Succeed to forward nobody@example.com
*Nov 15 12:23:54.559: VPDN MGR [uid:13]: accounting start sent
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:23:54.559: VPDN CALL [uid:13]: Connection succeeded
*Nov 15 12:23:54.559: SSS MGR [uid:13]: Handling Service-Connected event
*Nov 15 12:23:54.559: ppp13 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:23:54.559: [13]PPPoE 10: State LCP_NEGO    Event PPP_FWDED
*Nov 15 12:23:54.563: [13]PPPoE 10: data path set to SSS Switch
*Nov 15 12:23:54.563: [13]PPPoE 10: Connected Forwarded
```

Troubleshooting the Subscriber Service Switch on the LAC--Authorization Failure Example

The following is sample output indicating call failure due to authorization failure:

```
*Nov 15 12:37:24.535: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:37:24.535: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.539: PPPoE : encap string prepared
*Nov 15 12:37:24.539: [18]PPPoE 15: Access IE handle allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: pppoe SSS switch updated
*Nov 15 12:37:24.539: PPPoE 15: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:37:24.539: [18]PPPoE 15: AAA unique ID allocated
*Nov 15 12:37:24.539: [18]PPPoE 15: No AAA accounting method list
*Nov 15 12:37:24.539: [18]PPPoE 15: Service request sent to SSS
*Nov 15 12:37:24.539: [18]PPPoE 15: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:37:24.559: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:37:24.559: SSS INFO: Element type is Switch-Id, long value is -738197487
*Nov 15 12:37:24.559: SSS INFO: Element type is Nasport, ptr value is 63C0E590
*Nov 15 12:37:24.559: SSS INFO: Element type is AAA-Id, long value is 19
*Nov 15 12:37:24.559: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:24.559: SSS PM [uid:18]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:37:24.559: SSS PM [uid:18]: Received Service Request
*Nov 15 12:37:24.559: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy requires 'Unauth-User' key
*Nov 15 12:37:24.559: SSS PM [uid:18]: Policy reply - Need more keys
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Got reply Need-More-Keys from PM
*Nov 15 12:37:24.559: SSS MGR [uid:18]: Handling More-Keys event
*Nov 15 12:37:24.559: [18]PPPoE 15: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:37:24.559: [18]PPPoE 15: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:24.559: ppp18 PPP: Using default call direction
*Nov 15 12:37:24.559: ppp18 PPP: Treating connection as a dedicated line
*Nov 15 12:37:24.559: ppp18 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:37:24.559: ppp18 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:37:24.559: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.559: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:24.559: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:24.559: [18]PPPoE 15: State START_PPP    Event DYN_BIND
*Nov 15 12:37:24.559: [18]PPPoE 15: data path set to PPP
*Nov 15 12:37:24.563: ppp18 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
```

```
*Nov 15 12:37:24.563: ppp18 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:37:24.563: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:24.563: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:37:26.523: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.523: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.523: ppp18 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:37:26.527: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.527: ppp18 LCP:    MagicNumber 0x0023A93E (0x05060023A93E)
*Nov 15 12:37:26.575: ppp18 LCP: TIMEout: State ACKsent
*Nov 15 12:37:26.575: ppp18 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.575: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:37:26.575: ppp18 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:37:26.575: ppp18 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:37:26.575: ppp18 LCP:    MagicNumber 0xB0F8A971 (0x0506B0F8A971)
*Nov 15 12:37:26.575: ppp18 LCP: State is Open
*Nov 15 12:37:26.575: ppp18 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:37:26.575: ppp18 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:37:26.579: ppp18 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
Nov 15 12:37:26.579: ppp18 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:37:26.579: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Nov 15 12:37:26.579: SSS INFO: Element type is AccIe-Hdl, ptr value is 5B000011
*Nov 15 12:37:26.579: SSS INFO: Element type is AAA-Id, long value is 19
Nov 15 12:37:26.579: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:37:26.579: SSS MGR [uid:18]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:37:26.579: SSS PM [uid:18]: Received More Keys
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling Authorization Check
*Nov 15 12:37:26.579: SSS PM [uid:18]: Handling AAA service Authorization
*Nov 15 12:37:26.579: SSS PM [uid:18]: Sending authorization request for 'example.com'
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:Authorizing key example.com
*Nov 15 12:37:26.579: SSS AAA AUTHOR [uid:18]:AAA request sent for key example.com
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Received an AAA failure
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <service not found>, state
changed from authorizing to complete
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:No service authorization info found
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:37:26.587: SSS AAA AUTHOR [uid:18]:Free request
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Next Authorization Check
*Nov 15 12:37:26.587: SSS PM [uid:18]: Default policy: SGF author not needed
*Nov 15 12:37:26.587: SSS PM [uid:18]: Handling Default Service
*Nov 15 12:37:26.587: SSS PM [uid:18]: Policy reply - Local terminate
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Got reply Local-Term from PM
*Nov 15 12:37:26.591: SSS MGR [uid:18]: Handling Send-Client-Local-Term event
*Nov 15 12:37:26.591: ppp18 PPP: Phase is AUTHENTICATING, Unauthenticated User
Nov 15 12:37:26.595: ppp18 CHAP: O FAILURE id 1 len 25 msg is "Authentication
failed"
*Nov 15 12:37:26.599: ppp18 PPP: Sending Acct Event[Down] id[13]
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: ppp18 LCP: O TERMREQ [Open] id 3 len 4
*Nov 15 12:37:26.599: ppp18 LCP: State is Closed
*Nov 15 12:37:26.599: ppp18 PPP: Phase is DOWN
*Nov 15 12:37:26.599: ppp18 PPP: Phase is TERMINATING
*Nov 15 12:37:26.599: [18]PPPoE 15: State LCP_NEGO    Event PPP_DISCNCT
*Nov 15 12:37:26.599: [18]PPPoE 15: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:37:26.599: [18]PPPoE 15: AAA account stopped
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Processing a client disconnect
*Nov 15 12:37:26.599: SSS MGR [uid:18]: Handling Send-Service-Disconnect event
```

Troubleshooting the Subscriber Service Switch on the LAC--Authentication Failure Example

The following is sample output indicating call failure due to authentication failure at the LNS:

```
*Nov 15 12:45:02.067: PPPoE 0: I PADI R:0000.0c14.71d0 L:ffff.ffff.ffff 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE 0: O PADO R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE 0: I PADR R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.071: PPPoE : encap string prepared
*Nov 15 12:45:02.071: [21]PPPoE 18: Access IE handle allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: pppoe SSS switch updated
*Nov 15 12:45:02.071: PPPoE 18: AAA pppoe_aaa_acct_get_retrieved_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_nas_port_details
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:02.071: [21]PPPoE 18: AAA unique ID allocated
*Nov 15 12:45:02.071: [21]PPPoE 18: No AAA accounting method list
*Nov 15 12:45:02.071: [21]PPPoE 18: Service request sent to SSS
*Nov 15 12:45:02.071: [21]PPPoE 18: Created R:00b0.c2e9.c870 L:0000.0c14.71d0 1/32
ATM4/0.132
*Nov 15 12:45:02.091: SSS INFO: Element type is Access-Type, long value is 3
*Nov 15 12:45:02.091: SSS INFO: Element type is Switch-Id, long value is 1946157076
*Nov 15 12:45:02.091: SSS INFO: Element type is Nasport, ptr value is 63B34170
*Nov 15 12:45:02.091: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:02.091: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:02.091: SSS PM [uid:21]: RM/VPDN disabled: RM/VPDN author not needed
*Nov 15 12:45:02.091: SSS PM [uid:21]: Received Service Request
*Nov 15 12:45:02.091: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy requires 'Unauth-User' key
*Nov 15 12:45:02.091: SSS PM [uid:21]: Policy reply - Need more keys
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Got reply Need-More-Keys from PM
*Nov 15 12:45:02.091: SSS MGR [uid:21]: Handling More-Keys event
*Nov 15 12:45:02.091: [21]PPPoE 18: State REQ_NASPORT    Event MORE_KEYS
*Nov 15 12:45:02.091: [21]PPPoE 18: O PADS R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:02.091: ppp21 PPP: Using default call direction
*Nov 15 12:45:02.091: ppp21 PPP: Treating connection as a dedicated line
*Nov 15 12:45:02.091: ppp21 PPP: Phase is ESTABLISHING, Active Open
*Nov 15 12:45:02.091: ppp21 LCP: O CONFREQ [Closed] id 1 len 19
*Nov 15 12:45:02.091: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:02.091: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:02.091: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:02.091: [21]PPPoE 18: State START_PPP    Event DYN_BIND
*Nov 15 12:45:02.091: [21]PPPoE 18: data path set to PPP
*Nov 15 12:45:02.095: ppp21 LCP: I CONFREQ [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:    MRU 1492 (0x010405D4
*Nov 15 12:45:02.095: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.095: ppp21 LCP: O CONFACK [REQsent] id 1 len 14
*Nov 15 12:45:02.095: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:02.095: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:02.315:   Tnl41436 L2TP: I StopCCN from rp1 tnl 31166
*Nov 15 12:45:02.315:   Tnl41436 L2TP: Shutdown tunnel
*Nov 15 12:45:02.315:   Tnl41436 L2TP: Tunnel state change from no-sessions-left to
idle
*Nov 15 12:45:04.055: ppp21 LCP: I CONFREQ [ACKsent] id 2 len 14
*Nov 15 12:45:04.055: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.059: ppp21 LCP: O CONFACK [ACKsent] id 2 len 14
*Nov 15 12:45:04.059: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.059: ppp21 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
*Nov 15 12:45:04.079: ppp21 LCP: TIMEout: State ACKsent
*Nov 15 12:45:04.079: ppp21 LCP: O CONFREQ [ACKsent] id 2 len 19
*Nov 15 12:45:04.079: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
```

```
*Nov 15 12:45:04.079: ppp21 LCP: I CONFACK [ACKsent] id 2 len 19
*Nov 15 12:45:04.079: ppp21 LCP:    MRU 1492 (0x010405D4)
*Nov 15 12:45:04.079: ppp21 LCP:    AuthProto CHAP (0x0305C22305)
*Nov 15 12:45:04.079: ppp21 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
*Nov 15 12:45:04.079: ppp21 LCP: State is Open
*Nov 15 12:45:04.079: ppp21 PPP: Phase is AUTHENTICATING, by this end
*Nov 15 12:45:04.079: ppp21 CHAP: O CHALLENGE id 1 len 25 from "7200"
*Nov 15 12:45:04.083: ppp21 CHAP: I RESPONSE id 1 len 38 from "nobody@example.com"
*Nov 15 12:45:04.083: ppp21 PPP: Phase is FORWARDING, Attempting Forward
*Nov 15 12:45:04.083: SSS INFO: Element type is Unauth-User, string value is
nobody@example.com
*Nov 15 12:45:04.083: SSS INFO: Element type is AccIe-Hdl, ptr value is 71000014
*Nov 15 12:45:04.083: SSS INFO: Element type is AAA-Id, long value is 22
*Nov 15 12:45:04.083: SSS INFO: Element type is Access-Type, long value is 0
*Nov 15 12:45:04.083: SSS MGR [uid:21]: Handling Policy Authorize (1 pending
sessions)
*Nov 15 12:45:04.083: SSS PM [uid:21]: Received More Keys
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling Authorization Check
*Nov 15 12:45:04.083: SSS PM [uid:21]: Handling AAA service Authorization
*Nov 15 12:45:04.083: SSS PM [uid:21]: Sending authorization request for 'example.com'
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Event <make request>, state changed
from idle to authorizing
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:Authorizing key example.com
*Nov 15 12:45:04.083: SSS AAA AUTHOR [uid:21]:AAA request sent for key example.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Received an AAA pass
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <found service>, state changed
from authorizing to complete
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Found service info for key example.com
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Event <free request>, state changed
from complete to terminal
*Nov 15 12:45:04.095: SSS AAA AUTHOR [uid:21]:Free request
*Nov 15 12:45:04.095: SSS PM [uid:21]: Handling Service Direction
*Nov 15 12:45:04.095: SSS PM [uid:21]: Policy reply - Forwarding
*Nov 15 12:45:04.095: SSS MGR [uid:21]: Got reply Forwarding from PM
*Nov 15 12:45:04.099: SSS MGR [uid:21]: Handling Connect-Service event
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Event connect req, state changed from idle
to connecting
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Requesting connection
*Nov 15 12:45:04.099: VPDN CALL [uid:21]: Call request sent
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Event client connect, state changed from
idle to connecting
*Nov 15 12:45:04.099: VPDN MGR [uid:21]: Initiating compulsory connection to
192.168.8.2
*Nov 15 12:45:04.099:   Tnl/Sn31399/10 L2TP: Session FS enabled
*Nov 15 12:45:04.099:   Tnl/Sn31399/10 L2TP: Session state change from idle to
wait-for-tunnel
*Nov 15 12:45:04.099: uid:21  Tnl/Sn31399/10 L2TP: Create session
*Nov 15 12:45:04.099:   Tnl31399 L2TP: SM State idle
*Nov 15 12:45:04.099:   Tnl31399 L2TP: O SCCRQ
*Nov 15 12:45:04.099:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.099:   Tnl31399 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Nov 15 12:45:04.099:   Tnl31399 L2TP: SM State wait-ctl-reply
*Nov 15 12:45:04.099: [21]PPPoE 18: State LCP_NEGO    Event PPP_FWDING
*Nov 15 12:45:04.107:   Tnl31399 L2TP: I SCCRP from rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Got a challenge from remote peer, rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Got a response from remote peer, rp1
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Tunnel Authentication success
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Tunnel state change from wait-ctl-reply to
established
*Nov 15 12:45:04.107:   Tnl31399 L2TP: O SCCCN  to rp1 tnlid 9349
*Nov 15 12:45:04.107:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.107:   Tnl31399 L2TP: SM State established
*Nov 15 12:45:04.107: uid:21  Tnl/Sn31399/10 L2TP: O ICRQ to rp1 9349/0
*Nov 15 12:45:04.107: [21]PPPoE 18: Access IE nas port called
*Nov 15 12:45:04.107: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
wait-for-tunnel to wait-reply
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: O ICCN to rp1 9349/13589
*Nov 15 12:45:04.115:   Tnl31399 L2TP: Control channel retransmit delay set to 1
seconds
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
```

```
wait-reply to established
*Nov 15 12:45:04.115: uid:21  Tnl/Sn31399/10 L2TP: VPDN session up
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Event peer connected, state changed from
connecting to connected
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: Succeed to forward nobody@example.com
*Nov 15 12:45:04.115: VPDN MGR [uid:21]: accounting start sent
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Event connect ok, state changed from
connecting to connected
*Nov 15 12:45:04.115: VPDN CALL [uid:21]: Connection succeeded
*Nov 15 12:45:04.115: SSS MGR [uid:21]: Handling Service-Connected event
*Nov 15 12:45:04.115: ppp21 PPP: Phase is FORWARDED, Session Forwarded
*Nov 15 12:45:04.115: [21]PPPoE 18: State LCP_NEGO    Event PPP_FWDED
*Nov 15 12:45:04.115: [21]PPPoE 18: data path set to SSS Switch
*Nov 15 12:45:04.119: [21]PPPoE 18: Connected Forwarded
*Nov 15 12:45:04.119: ppp21 PPP: Process pending packets
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Result code(2): 2: Call
disconnected, refer to error msg
*Nov 15 12:45:04.139:      Error code(6): Vendor specific
*Nov 15 12:45:04.139:      Optional msg: Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: I CDN from rp1 tnl 9349, cl
13589
01:06:21: %VPDN-6-CLOSED: L2TP LNS 192.168.8.2 closed  user nobody@example.com; Result
2, Error 6, Locally generated disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: disconnect (L2X) IETF:
18/host-request Ascend: 66/VPDN Local PPP Disconnect
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Destroying session
*Nov 15 12:45:04.139: uid:21  Tnl/Sn31399/10 L2TP: Session state change from
established to idle
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Event peer disconnect, state changed from
connected to disconnected
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: Remote disconnected nobody@example.com
*Nov 15 12:45:04.139: VPDN MGR [uid:21]: accounting stop sent
*Nov 15 12:45:04.139:   Tnl31399 L2TP: Tunnel state change from established to
no-sessions-left
*Nov 15 12:45:04.143:   Tnl31399 L2TP: No more sessions in tunnel, shutdown (likely)
in 15 seconds
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event server disc, state changed from
connected to disconnected
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Server disconnected call
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Event free req, state changed from
disconnected to terminal
*Nov 15 12:45:04.143: VPDN CALL [uid:21]: Free request
*Nov 15 12:45:04.143: SSS MGR [uid:21]: Handling Send Client Disconnect
*Nov 15 12:45:04.143: [21]PPPoE 18: State CNCT_FWDED    Event SSS_DISCNCT
*Nov 15 12:45:04.143: ppp21 PPP: Sending Acct Event[Down] id[16]
*Nov 15 12:45:04.143: ppp21 PPP: Phase is TERMINATING
*Nov 15 12:45:04.143: ppp21 LCP: State is Closed
*Nov 15 12:45:04.143: ppp21 PPP: Phase is DOWN
*Nov 15 12:45:04.143: [21]PPPoE 18: O PADT R:0000.0c14.71d0 L:00b0.c2e9.c870 1/32
ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: Destroying R:0000.0c14.71d0 L:00b0.c2e9.c870
1/32 ATM4/0.132
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA pppoe_aaa_acct_get_dynamic_attrs
*Nov 15 12:45:04.143: [21]PPPoE 18: AAA account stopped
*Nov 15 12:45:14.139:   Tnl31399 L2TP: I StopCCN from rp1 tnl 9349
*Nov 15 12:45:14.139:   Tnl31399 L2TP: Shutdown tunnel
*Nov 15 12:45:14.139:   Tnl31399 L2TP: Tunnel state change from no-sessions-left
```

Troubleshooting the Subscriber Service Switch on the LNS--Normal Operation Example

The following example shows the **debug** commands used and sample output indicating normal operation of the Subscriber Service Switch on the LNS:

```
Router# debug sss event
Router# debug sss error
Router# debug sss fsm
Router# debug ppp negotiation
Router# debug vpdn l2x-events
```

```
Router# debug vpdn l2x-errors
Router# debug vpdn sss events
Router# debug vpdn sss errors
Router# debug vpdn sss fsm
SSS:
  SSS events debugging is on
  SSS error debugging is on
  SSS fsm debugging is on
PPP:
  PPP protocol negotiation debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN SSS events debugging is on
  VPDN SSS errors debugging is on
  VPDN SSS FSM debugging is on
3d17h:   Tnl9264 L2TP: I ICRQ from server1 tnl 61510
3d17h:   Tnl/Sn9264/13586 L2TP: Session FS enabled
3d17h:   Tnl/Sn9264/13586 L2TP: Session state change from idle to wait-connect
3d17h:   Tnl/Sn9264/13586 L2TP: New session created
3d17h:   Tnl/Sn9264/13586 L2TP: O ICRP to server1 61510/7
3d17h:   Tnl9264 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl/Sn9264/13586 L2TP: I ICCN from server1 tnl 61510, cl 7
3d17h: nobody@example.com  Tnl/Sn9264/13586 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:707]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is 1493172561
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1
3d17h: SSS INFO: Element type is AAA-Id, long value is 16726
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is D1000167
3d17h: SSS MGR [uid:707]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:707]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:707]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:707]: Multihop disabled: SGF author not needed
3d17h: SSS PM [uid:707]: No more authorization methods left to try, providing
default service
3d17h: SSS PM [uid:707]: Received Service Request
3d17h: SSS PM [uid:707]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:707]: Handling Service Direction
3d17h: SSS PM [uid:707]: Policy reply - Local terminate
3d17h: SSS MGR [uid:707]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:707]: Event policy-connect local, state changed from
wait-for-auth to connected
3d17h: SSS MGR [uid:707]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from SSS to PPP
3d17h: ppp707 PPP: Phase is ESTABLISHING
3d17h: ppp707 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp707 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp707 LCP:    AuthProto CHAP (0x0305C22305)
3d17h: ppp707 LCP:    MagicNumber 0xB0EC4557 (0x0506B0EC4557)
3d17h: ppp707 LCP: I FORCED sent CONFACK len 10
3d17h: ppp707 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp707 LCP:    MagicNumber 0x0017455D (0x05060017455D)
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp707 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp707 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:707]: Event connect local, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event vaccess resp, state changed from PPP to PPP
3d17h: VPDN SSS [Vi4.2]: Event stat bind resp, state changed from PPP to CNCT
3d17h: Vi4.2  Tnl/Sn9264/13586 L2TP: Session state change from
wait-for-service-selection to established
3d17h: Vi4.2 PPP: Phase is AUTHENTICATING, Authenticated User
3d17h: Vi4.2 CHAP: O SUCCESS id 1 len 4
3d17h: Vi4.2 PPP: Phase is UP
3d17h: Vi4.2 IPCP: O CONFREQ [Closed] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 172.16.0.0 (0x030681010000)
3d17h: Vi4.2 PPP: Process pending packets
```

```
3d17h: Vi4.2 IPCP: I CONFREQ [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 10.0.0.0 (0x030600000000)
3d17h: Vi4.2 AAA/AUTHOR/IPCP: Start.  Her address 10.0.0.0, we want 10.0.0.0
3d17h: Vi4.2 AAA/AUTHOR/IPCP: Done.  Her address 10.0.0.0, we want 10.0.0.0
3d17h: Vi4.2 IPCP: Pool returned 10.1.1.3
3d17h: Vi4.2 IPCP: O CONFNAK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: I CONFACK [REQsent] id 1 len 10
3d17h: Vi4.2 IPCP:    Address 172.16.0.0 (0x030681010000)
3d17h: Vi4.2 IPCP: I CONFREQ [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: O CONFACK [ACKrcvd] id 2 len 10
3d17h: Vi4.2 IPCP:    Address 10.1.1.3 (0x03065B010103)
3d17h: Vi4.2 IPCP: State is Open
3d17h: Vi4.2 IPCP: Install route to 10.1.1.3
```

Troubleshooting the Subscriber Service Switch on the LNS--Tunnel Failure Example

The following is sample output indicating tunnel failure on the LNS:

```
3d17h: L2TP: I SCCRQ from server1 tnl 31399
3d17h:   Tnl9349 L2TP: Got a challenge in SCCRQ, server1
3d17h:   Tnl9349 L2TP: New tunnel created for remote server1, address 192.168.8.1
3d17h:   Tnl9349 L2TP: O SCCRP  to server1 tnlid 31399
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl9349 L2TP: Tunnel state change from idle to wait-ctl-reply
3d17h:   Tnl9349 L2TP: I SCCCN from server1 tnl 31399
3d17h:   Tnl9349 L2TP: Got a Challenge Response in SCCCN from server1
3d17h:   Tnl9349 L2TP: Tunnel Authentication success
3d17h:   Tnl9349 L2TP: Tunnel state change from wait-ctl-reply to established
3d17h:   Tnl9349 L2TP: SM State established
3d17h:   Tnl9349 L2TP: I ICRQ from server1 tnl 31399
3d17h:   Tnl/Sn9349/13589 L2TP: Session FS enabled
3d17h:   Tnl/Sn9349/13589 L2TP: Session state change from idle to wait-connect
3d17h:   Tnl/Sn9349/13589 L2TP: New session created
3d17h:   Tnl/Sn9349/13589 L2TP: O ICRP to server1 31399/10
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl/Sn9349/13589 L2TP: I ICCN from server1 tnl 31399, cl 10
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Session state change from
wait-connect to wait-for-service-selection
3d17h: VPDN SSS []: Event start sss, state changed from IDLE to SSS
3d17h: VPDN SSS [uid:709]: Service request sent to SSS
3d17h: SSS INFO: Element type is Access-Type, long value is 4
3d17h: SSS INFO: Element type is Switch-Id, long value is -1912602284
3d17h: SSS INFO: Element type is Tunnel-Name, string value is server1
3d17h: SSS INFO: Element type is Can-SIP-Redirect, long value is 1
3d17h: SSS INFO: Element type is AAA-Id, long value is 16729
3d17h: SSS INFO: Element type is AccIe-Hdl, ptr value is 8D00016A
3d17h: SSS MGR [uid:709]: Event service-request, state changed from wait-for-req to
wait-for-auth
3d17h: SSS MGR [uid:709]: Handling Policy Authorize (1 pending sessions)
3d17h: SSS PM [uid:709]: RM/VPDN disabled: RM/VPDN author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: AAA author not needed
3d17h: SSS PM [uid:709]: Multihop disabled: SGF author not needed
d17h: SSS PM [uid:709]: No more authorization methods left to try, providing default
service
3d17h: SSS PM [uid:709]: Received Service Request
3d17h: SSS PM [uid:709]: Event <found>, State: initial-req to end
3d17h: SSS PM [uid:709]: Handling Service Direction
3d17h: SSS PM [uid:709]: Policy reply - Local terminate
3d17h: SSS MGR [uid:709]: Got reply Local-Term from PM
3d17h: SSS MGR [uid:709]: Event policy-connect local, state changed from
wait-for-auth to connected
3d17h: SSS MGR [uid:709]: Handling Send-Client-Local-Term event
3d17h: VPDN SSS [uid:709]: Event connect local, state changed from SSS to PPP
3d17h: ppp709 PPP: Phase is ESTABLISHING
3d17h: ppp709 LCP: I FORCED rcvd CONFACK len 15
3d17h: ppp709 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp709 LCP:    AuthProto CHAP (0x0305C22305)
3d17h: ppp709 LCP:    MagicNumber 0xB0FFA4D8 (0x0506B0FFA4D8)
3d17h: ppp709 LCP: I FORCED sent CONFACK len 10
```

```
3d17h: ppp709 LCP:    MRU 1492 (0x010405D4)
3d17h: ppp709 LCP:    MagicNumber 0x002AA481 (0x0506002AA481)
3d17h: ppp709 PPP: Phase is FORWARDING, Attempting Forward
3d17h: VPDN SSS [uid:709]: Event dyn bind resp, state changed from PPP to PPP
3d17h: ppp709 PPP: Phase is AUTHENTICATING, Unauthenticated User
3d17h: ppp709 CHAP: O FAILURE id 1 len 25 msg is "Authentication failed"
3d17h: ppp709 PPP: Sending Acct Event[Down] id[4159]
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: ppp709 LCP: O TERMREQ [Open] id 1 len 4
3d17h: ppp709 LCP: State is Closed
3d17h: ppp709 PPP: Phase is DOWN
3d17h: ppp709 PPP: Phase is TERMINATING
3d17h: VPDN SSS [uid:709]: Event peer disc, state changed from PPP to DSC
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: disconnect (AAA) IETF:
17/user-error Ascend: 26/PPP CHAP Fail
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: O CDN to server1 31399/10
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Destroying session
3d17h: nobody@example.com  Tnl/Sn9349/13589 L2TP: Session state change from
wait-for-service-selection to idle
3d17h: VPDN SSS [uid:709]: Event vpdn disc, state changed from DSC to END
3d17h:   Tnl9349 L2TP: Tunnel state change from established to no-sessions-left
3d17h:   Tnl9349 L2TP: No more sessions in tunnel, shutdown (likely) in 10 seconds
3d17h: SSS MGR [uid:709]: Processing a client disconnect
3d17h: SSS MGR [uid:709]: Event client-disconnect, state changed from connected to
end
3d17h: SSS MGR [uid:709]: Handling Send-Service-Disconnect event
3d17h:   Tnl9349 L2TP: O StopCCN  to server1 tnlid 31399
3d17h:   Tnl9349 L2TP: Control channel retransmit delay set to 1 seconds
3d17h:   Tnl9349 L2TP: Tunnel state change from no-sessions-left to shutting-down
3d17h:   Tnl9349 L2TP: Shutdown tunnel
```

Where to Go Next

- If you want to establish PPPoE session limits for sessions on a specific permanent virtual circuit or VLAN configured on an L2TP access concentrator, refer to the "Establishing PPPoE Session Limits per NAS Port" module.
- If you want to use service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup, refer to the "Offering PPPoE Clients a Selection of Services During Call Setup" module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over a L2TP control channel to an LNS or tunnel switch, refer to the "Enabling PPPoE Relay Discovery and Service Selection Functionality" module.
- If you want to configure a transfer upstream of the PPPoX session speed value, refer to the "Configuring Upstream Connections Speed Transfer" module.
- If you want to use the Simple Network Management Protocol (SNMP) to monitor PPPoE sessions, refer to the "Monitoring PPPoE Sessions with SNMP" module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, refer to the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, see the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

The following sections provide references related to configuring Cisco Subscriber Service Switch policies.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation module
Tasks for preparing for broadband access aggregation.	Preparing for Broadband Access Aggregation module
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Configuration procedure for PPPoE.	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions
Configuration procedures for PPPoA.	Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Standards

Standards	Title
None	--

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Configuring a Subscriber Service Switch Policy

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

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

Table 16 Feature Information for Configuring a Cisco Subscriber Service Switch Policy

Feature Name	Releases	Feature Configuration Information
Subscriber Service Switch	Cisco IOS XE Release 2.1	The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers, and how to define the services. The primary purpose of the Subscriber Service Switch is to direct PPP from one point to another using a Layer 2 subscriber policy. This feature was integrated into Cisco IOS XE Release 2.1.

Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS

The Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS feature enables you to shape PPP over Ethernet over VLAN sessions to a user-specified rate. The router shapes the sum of all of the traffic to the PPPoE session so that the subscriber's connection to the digital subscriber line access multiplexer (DSLAM) does not become congested. Queueing-related functionality provides different levels of service to the various applications that execute over the PPPoE session.

A nested, two-level hierarchical service policy is used to configure session shaping directly on the router using the modular quality of service command-line interface (MQC). The RADIUS server applies the service policy to a particular PPPoE session by downloading a RADIUS attribute to the router. This attribute specifies the policy map name to apply to the session. RADIUS notifies the router to apply the specified policy to the session. Because the service policy contains queueing-related actions, the router sets up the appropriate class queues and creates a separate versatile traffic management and shaping (VTMS) system link dedicated to the PPPoE session.

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 Table at the end of this document.

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

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 150
- How RADIUS Uses VSA 38 in User Profiles, page 151
- Commands Used to Define QoS Actions, page 151

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, page 150 for QoS policy definitions.

Commands Used to Define QoS Actions

When you configure queueing and shaping for PPPoE over VLAN sessions, the child policy of a nested hierarchical service policy defines QoS actions using any of the following QoS commands:

- **priority** command--Assigns priority to a traffic class and gives preferential treatment to the class.
- **bandwidth** command--Enables class-based fair queueing and creates multiple class queues based on bandwidth.
- **queue-limit** command--Specifies the maximum number of packets that a particular class queue can hold.

- **police** command--Regulates traffic based on bits per second (bps), using the committed information rate (CIR) and the peak information rate, or on the basis of a percentage of bandwidth available on an interface.
- **random-detect** command--Drops packets based on a specified value to control congestion before a queue reaches its queue limit. The drop policy is based on IP precedence, differentiated services code point (DSCP), or the discard-class.
- **set ip precedence** command--Marks a packet with the IP precedence level you specify.
- **set dscp** command--Marks a packet with the DSCP you specify.
- **set cos** command--Sets the IEEE 802.1Q class of service bits in the user priority field.

The parent policy contains only the class-default class with the **shape** command configured. This command shapes traffic to the specified bit rate, according to a specific algorithm.

The router allows you to apply QoS policy maps using RADIUS. The actual configuration of the policy map occurs on the router using the MQC. The router can apply the QoS policy to sessions using attributes defined in one of the following RADIUS profiles:

- User Profile--The user profile on the RADIUS server contains an entry that identifies the policy map name applicable to the user. The policy map name is the service that RADIUS downloads to the router after a session is authorized.
- Service Profile--The service profile on the RADIUS server specifies a session identifier and an attribute-value (AV) pair. The session identifier might be, for example, the IP address of the session. The AV-pair defines the service (policy map name) to which the user belongs.

The following AV-pairs define the QoS policy to be applied dynamically to the session:

"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"

"ip:sub-qos-policy-out=<name of egress policy>"

When RADIUS gets a service-logon request from the policy server, it sends a change of authorization (CoA) request to the router to activate the service for the subscriber, who is already logged in.

If the authorization succeeds, the router downloads the name of the policy map from RADIUS using the above attribute and applies the QoS policy to the session.

Note Although the router also supports the RADIUS vendor specific attribute (VSA) 38, Cisco-Policy-Down and Cisco-Policy-Up, we recommend that you use the above attributes for QoS policy definitions.

How to Use the Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS Feature

Configuring a Per Session Queueing and Shaping Policy on the Router

To configure a per session queueing and shaping policy on the router for PPPoE over VLAN sessions using RADIUS, you must complete the following steps.

SUMMARY STEPS

1. **policy-map** *policy-map-name*
2. **class**
3. **bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} **account**{{**qinq**| **dot1q**} {**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}}
4. exit
5. **policy-map** *policy-map-name*
6. **class** *class-default*
7. **shape** *rate* **account** {{{**qinq**| **dot1q**}{**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}}
8. **service-policy** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map policy-map-name`	Creates or modifies the bottom-level child policy. • *policy-map-name* is the name of the child policy map. The name can be a maximum of 40 alphanumeric characters.
Step 2	**class** **Example:** `Router(config-pmap)# class class-map-name`	Assigns the traffic class you specify to the policy map. Enters policy-map class configuration mode. • *class-map-name* is the name of a previously configured class map and is the traffic class for which you want to define QoS actions. • Repeat Steps 2 and 3 for each traffic class you want to include in the policy map.

	Command or Action	Purpose
Step 3	**bandwidth** {*bandwidth-kbps* | **percent** *percentage* | **remaining percent** *percentage*} **account**{{**qinq**| **dot1q**} {**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}} **Example:** `Router(config-pmap-c)# bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {aal5 | aal3} subscriber-encapsulation | user-defined offset [atm]}`	Enables class-based fair queueing. • *bandwidth-kbps* specifies or modifies the minimum bandwidth allocated for a class belonging to a policy map. Valid values are from 8 to 2488320, which represents from 1 to 99 percent of the link bandwidth. • **percent** *percentage* specifies or modifies the minimum percentage of the link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **remaining percent** *percentage* specifies or modifies the minimum percentage of unused link bandwidth allocated for a class belonging to a policy map. Valid values are from 1 to 99. • **account** enables ATM overhead accounting. For more information, see the " ATM Overhead Accounting " section of the "Configuring Dynamic Subscriber Services" chapter of the *Cisco 10000 Series Router Quality of Service Configuration Guide*. • **qinq** specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **dot1q** specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **aal5** specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. You must specify either **aal5** or aal3. • **aal3** specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**. • *subscriber-encapsulation* specifies the encapsulation type at the subscriber line. • **user-defined** indicates that the router is to use the *offset* you specify when calculating ATM overhead. • *offset* specifies the offset size the router is to use when calculating ATM overhead. Valid values are from -63 to 63 bytes. **Note** The router configures the offset size if you do not specify the *offset* option. • **atm** applies ATM cell tax in the ATM overhead calculation.
Step 4	exit **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

	Command or Action	Purpose
Step 5	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map policy-map-name`	Creates or modifies the parent policy. • *policy-map-name* is the name of the parent policy map. The name can be a maximum of 40 alphanumeric characters.
Step 6	**class** *class-default* **Example:** `Router(config-pmap)# class class-default`	Configures or modifies the parent class-default class. **Note** You can configure only the class-default class in a parent policy. Do not configure any other traffic class.
Step 7	**shape** *rate* **account** {{{**qinq**| **dot1q**} {**aal5**| **aal3**} {*subscriber-encapsulation*}} | {**user-defined** *offset* [**atm**]}} **Example:** `Router(config-pmap-c)# shape rate account {qinq | dot1q} {aal5 | aal3} subscriber-encapsulation | {user-defined offset [atm]}`	Shapes traffic to the indicated bit rate and enables ATM overhead accounting. • *rate* is the bit-rate used to shape the traffic, expressed in kilobits per second. • **account** enables ATM overhead accounting. • **qinq** specifies queue-in-queue encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **dot1q** specifies IEEE 802.1Q VLAN encapsulation as the broadband aggregation system-DSLAM encapsulation type. • **aal5** specifies the ATM Adaptation Layer 5 that supports connection-oriented VBR services. You must specify either **aal5** or **aal3**. • **aal3** specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**. • *subscriber-encapsulation* specifies the encapsulation type at the subscriber line. • **user-defined** indicates that the router is to use the *offset* you specify when calculating ATM overhead. • *offset* specifies the offset size the router is to use when calculating ATM overhead. Valid values are from -63 to 63 bytes. **Note** The router configures the offset size if you do not specify the **user-defined** *offset* option. • **atm** applies ATM cell tax in the ATM overhead calculation.
Step 8	**service-policy** *policy-map-name* **Example:** Router(config-pmap-c)# **service-policy** *policy-map-name*	Applies a bottom-level child policy to the top-level parent class-default class. • *policy-map-name* is the name of the previously configured child policy map.

Verifying Per Session Queueing

To display the configuration of per session queueing and shaping policies for PPPoE over VLAN, enter any of the following commands in privileged EXEC mode:

Command	Purpose
`Router#` **show policy-map interface interface**	Displays information about the policy map attached to the interface you specify. If you do not specify an interface, it displays information about all of the policy maps configured on the router. • *interface* specifies the virtual-access interface and number the router created for the session (for example, virtual-access 1).
`Router#` **show policy-map session uid** `uid-number`	Displays the session QoS counters for the subscriber session you specify. • **uid** *uid-number* defines a unique session ID. Valid values for *uid-number* are from 1 to 65535.
`Router#` **show running-config**	Displays the running configuration on the router. The output shows the AAA setup and the configuration of the policy map, ATM VC, PPPoA, dynamic bandwidth selection, virtual template, and RADIUS server.

Configuration Examples for Per Session Queueing and Shaping Policies

Configuring a Per Session Queueing and Shaping Policy on the Router Example

The following example shows

The example creates two traffic classes: Voice and Video. The router classifies traffic that matches IP precedence 5 as Voice traffic and traffic that matches IP precedence 3 as Video traffic. The Child policy map gives priority to Voice traffic and polices traffic at 2400 kbps. The Video class is allocated 80 percent of the remaining bandwidth and has ATM overhead accounting enabled. The Child policy is applied to the class-default class of the Parent policy map, which receives 20 percent of the remaining bandwidth and shapes traffic to 10,000 bps, and has ATM overhead accounting enabled.

```
Router(config)# class-map Voice
```

```
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# class-map Video
Router(config-cmap)# match ip precedence 3
!
Router(config)# policy-map Child
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# police 2400 9216 0 conform-action transmit exceed-action drop
violate-action drop
Router(config-pmap-c)# class video
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-dot1q-rbe
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 10000 account dot1q snap-dot1q-rbe
Router(config-pmap-c)# service-policy Child
```

Setting Up RADIUS for Per Session Queueing and Shaping Example

The following are example configurations for the Merit RADIUS server and the associated Layer 2 network server (LNS). In the example, the Cisco-Policy-Down attribute indicates the name of the policy map to be downloaded, which in this example is rad-output-policy. The RADIUS dictionary file includes an entry for Cisco VSA 38.

```
example.com Password = "cisco123"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Cisco:Cisco-Policy-Down = rad-output-policy
```

Cisco.attr Cisco-Policy-Up 37 string (*, *)

Cisco.attr Cisco-Policy-Down 38 string (*, *)

Verifying Per Session Queueing and Shaping Policies Examples

This example shows sample output for the **show policy-map interface** command

```
Router#
!
!
Service-policy output: TEST
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 100/1000
```

This example shows sample output from the **show policy-map session** command and **show policy-map session uid** command, based on a nested hierarchical policy.

```
Router# show subscriber session
Current Subscriber Information: Total sessions 1
Uniq ID Interface  State         Service      Identifier           Up-time
36      Vi2.1      authen        Local Term   peapen@cisco.com     00:01:36
Router# show policy-map parent
  Policy Map parent
    Class class-default
      Average Rate Traffic Shaping
```

```
      cir 10000000 (bps)
      service-policy child
Router# show policy-map child

  Policy Map child
    Class voice
      priority
      police 8000 9216 0
       conform-action transmit
       exceed-action drop
       violate-action drop
    Class video
      bandwidth remaining 80 (%)
Router# show policy-map session uid 36
 SSS session identifier 36 -
 SSS session identifier 36 -
  Service-policy output: parent
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
      Service-policy : child
        queue stats for all priority classes:
          Queueing
          queue limit 16 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: voice (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 5
          Priority: Strict, burst bytes 1500, b/w exceed drops: 0

          Police:
            8000 bps, 9216 limit, 0 extended limit
            conformed 0 packets, 0 bytes; action:
            transmit
            exceeded 0 packets, 0 bytes; action:
            drop
            violated 0 packets, 0 bytes; action:
            drop
        Class-map: video (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 3
          Queueing
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth remaining 80% (7993 kbps)
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
          queue limit 250 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 2/136
```

Additional References

The following sections provide references related to the Per Session Queueing and Shaping for PPPoEoVLAN Using RADIUS feature.

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

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

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

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

Table 17 Feature Information for Per Session Queueing and Shaping for PPPoE over VLAN Using RADIUS

Feature Name	Releases	Feature Information
Per Session Queueing and Shaping for PPPoE over VLAN Using RADIUS	Cisco IOS XE Release 2.1	This feature enables you to shape PPPoE over VLAN sessions to a user-specified rate. The Per Session Queueing and Shaping for PPPoE over VLAN Support Using RADIUS feature was introduced on the PRE2 to enable dynamic queueing and shaping policies on PPPoEoVLAN session. This feature was integrated into Cisco IOS XE Release 2.1.

802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization. This capability enables a way to provide best-effort quality of service (QoS) or class of service (CoS) at Layer 2 without requiring reservation setup.

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 Table at the end of this document.

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

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

The PPPoE over 802.1Q VLAN feature must be enabled.

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

You cannot set different CoS levels for PPP and Point-to-Point Protocol over Ethernet (PPPoE) control packets; all control packets default to a CoS level set at 0.

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

To configure the 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature, you should understand the following concepts:

The command can help troubleshoot 802.1P control frame marking: **debug pppoe error**

Benefits of 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature facilitates moving from ATM-based to Ethernet-based networks by supporting the ability to offer prioritized traffic services, Voice over Internet Protocol (VoIP), and other premium services.

Feature Design of 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The IEEE 802.1P specification is an extension of the IEEE 802.1Q VLANs tagging standard and enables Layer 2 devices to prioritize traffic by using an 802.1P header that includes a three-bit user priority field. If congestion occurs when the 802.1P CoS bit is not set, PPP keepalive packets can be lost, which can result in disconnection of an established session with loss of service to the end user. Congestion caused by noncontrol packets can also prevent new sessions from being established, which also can result in denying service to the end user.

PPPoE sessions established over 802.1Q VLANs use the priority header field to provide best-effort QoS or CoS at Layer 2 without involving reservation setup. 802.1P traffic is marked and sent to the destination, and no bandwidth reservations are established.

In Cisco IOS XE Release 2.4, PPPoE sessions established over IEEE 802.1Q VLAN make use of the priority field of the IEEE 802.1p header by setting the CoS field to user priority 7.

During network congestion, when the Ethernet network and digital subscriber line access multiplexer (DSLAM) offer 802.1P support, control packets are offered a higher priority than noncontrol packets, thereby increasing the likelihood of reliable delivery. PPPoE control packets and PPP packets originating from the broadband remote access server (BRAS) are marked with user priority 0, the highest level of priority.

The following packets are tagged with user priority 0 in their 802.1P header:

- PPPoE packets
  - PPPoE Active Discovery Offer (PADO)
  - PPPoE Active Discovery Session Confirmation (PADS)

- PPP packets
    - Link Control Protocol (LCP)
    - Network Control Protocol (NCP) (Internet Protocol Control Protocol (IPCP))
    - Authentication
    - Keepalive

How to Configure 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature is enabled by default and requires no configuration.

Configuration Examples for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

The following task explains how to change the CoS setting for PPP and PPPoE control frames over 802.1Q VLAN.

- Setting 802.1P Priority Bits in 802.1Q Frames Containing PPPoE Control Packets, page 163

Setting 802.1P Priority Bits in 802.1Q Frames Containing PPPoE Control Packets

This task explains how to change the CoS settings for PPP and PPPoE control frames over 802.1Q VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **control-packets vlan cos priority**
5. **exit**
6. **bba-group pppoe group-name**
7. **control-packets vlan cos priority**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe global`	Specifies the BBA group and enters BBA group configuration mode.
Step 4	**control-packets vlan cos priority** **Example:** `Router(config-bba-group)# control-packets vlan cos 5`	Sets the PPPoE control packets associated with the BBA group.
Step 5	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode, and returns to global configuration mode.
Step 6	**bba-group pppoe group-name** **Example:** `Router(config)# bba-group pppoe cisco`	Specifies the BBA group cisco and enters BBA group configuration mode.
Step 7	**control-packets vlan cos priority** **Example:** `Router(config-bba-group)# control-packets vlan cos 2`	Sets the PPPoE control packets associated with the BBA group.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode, and returns to global configuration mode.

Additional References

The following sections provide references related to the 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	*Cisco IOS XE Broadband and DSL Configuration Guide*
Broadband access commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

Standard	Title
IEEE Standard 802.1P	PPPoE over IEEE 802.1Q
IEEE Standard 802.1Q	Virtual Bridged Local Area Networks

MIBs

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

RFCs

RFC	Title
RFC 2516	PPP over Ethernet

Technical Assistance

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

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

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

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

Table 18 Feature Information for 802.1P CoS Bit Set for PPP and PPPoE Control Frames

Feature Name	Releases	Feature Information
802.1P CoS Bit Set for PPP and PPPoE Control Frames	Cisco IOS XE Release 2.4	The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization. This capability enables a way to provide best-effort QoS or CoS at Layer 2 without requiring reservation setup. In Cisco IOS XE Release 2.4, this feature was introduced. The following command was introduced: **control-packets vlan cos**.

PPPoE Smart Server Selection

The PPPoE Smart Server Selection feature allows service providers to determine which Broadband Remote Access Server (BRAS) a PPP call will terminate on.

The PPPoE Smart Server Selection feature allows you to configure a specific PPP over Ethernet (PPPoE) Active Discovery Offer (PADO) delay for a received PPPoE Active Discovery Initiation (PADI) packet. The PADO delay establishes the order in which the BRASs respond to PADIs by delaying their responses to particular PADIs by various times.

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 Table at the end of this document.

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

Information About PPPoE Smart Server Selection

Benefits of PPPoE Smart Server Selection

PPPoE Smart Server Selection provides the following benefits for the Internet service providers (ISPs):

- Optimize their networks by predicting and isolating PPP calls to terminate on a particular BRAS.
- Establish a priority order among the BRASs by configuring varying degrees of delays in the broadband access (BBA) groups on different BRASs.
- Use circuit ID and remote ID tag matching with strings up to 64 characters in length.

- Use spaces in remote ID, circuit ID, and PPPoE service names.
- Restrict the service advertisements from a BRASs in a PADO message.
- Apply a PADO transmission delay based on circuit ID, remote ID, and service name.
- Do partial matching on service name, remote ID, and circuit ID.

How to Configure PPPoE Smart Server Selection

- Configuring BBA Group PADO Delay, page 170
- Configuring PADO Delay Based on Remote ID or Circuit ID, page 171
- Configuring PPPoE Service PADO Delay, page 174

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*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe server-selection`	Defines a PPP over Ethernet (PPPoE) profile, and enters BBA group configuration mode. • The **global** keyword creates a profile, which serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**pado delay** *milliseconds* **Example:** `Router(config-bba-group)# pado delay 45`	Sets the time by which a PADO response is delayed for a BBA group. **Note** Setting a value of 0 means no transmission delay. Setting a value of 9999 means setting an infinite time (PADO is never sent).

• Troubleshooting Tips, page 171

Troubleshooting Tips

Use the **debug pppoe** command to troubleshoot the PPPoE session.

Configuring PADO Delay Based on Remote ID or Circuit ID

This task uses the **pppoe server** command to define a list of circuit ID and remote ID tags on a BRAS for a particular BBA group. The **pppoe delay** command is extended to specify delays based on the PPPoE circuit ID or remote ID tag.

All incoming calls are scanned and if the circuit ID or remote ID tags in the PADI match the list on the BRAS, then the PADO response will be delayed by the configured delay time. If there is no delay defined based on the circuit ID or remote ID, the per-PPPoE service delay is sought. It it is not found, the delay for the BBA group PADO is used. If no PPPoE delay is found, the PADO is sent without delay.

If there is no match and a BBA group PADO delay is configured under the same BBA group, then the PADO response is delayed by the configured delay time for that BBA group. If a BBA group PADO delay is not configured, then the PADO response is sent immediately.

With PPPoE smart server selection, you can do a partial match for a configured string by using a circuit ID or remote ID delay configured for the PPPoE server. (*Partial matching* is searching for parts of strings. It is used to search for similar strings.) The preference for matching the string is described in the Configuring PADO Delay Based on Remote ID or Circuit ID, page 171 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name*| **global**}
4. **pppoe server circuit-id delay** *milliseconds* **string** [**contains**] *circuit-id-string*
5. **pppoe server remote-id delay** *milliseconds* **string** [**contains**] *remote-id-string*
6. **pado delay circuit-id** *milliseconds*
7. **pado delay remote-id** *milliseconds*
8. **pado delay** *milliseconds*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name*| **global**} **Example:** `Router(config)# bba-group pppoe server-selection`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port.
Step 4	**pppoe server circuit-id delay** *milliseconds* **string** [**contains**] *circuit-id-string* **Example:** `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. • The **contains** keyword can find a partial match for this delay statement. • The value for the *circuit-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, "circuit ATM1/0/0 VC 0/100").

	Command or Action	Purpose
Step 5	**pppoe server remote-id delay** *milliseconds* **string** [**contains**] *remote-id-string* **Example:** `Router(config-bba-group)# pppoe server remote-id delay 30 string XTH-TEST` **Example:**	(Optional) Specifies the delay to be applied based on the PPPoE tag remote ID from the client. • The **contains** keyword can find a partial match for this delay statement. • The value for the *remote-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, "subscr mac 1111.2222.3333").
Step 6	**pado delay circuit-id** *milliseconds* **Example:** `Router(config-bba-group)# pado delay circuit-id 35`	(Optional) Finds a match based on the PPPoE group circuit ID delay if configured. • If a circuit ID cannot be matched partially, a delay is applied based on any circuit ID that is present.
Step 7	**pado delay remote-id** *milliseconds* **Example:** `Router(config-bba-group)# pado delay remote-id 30`	(Optional) Finds a match based on the PPPoE group remote ID delay if configured.
Step 8	**pado delay** *milliseconds* **Example:** `Router(config-bba-group)# pado delay 45`	(Optional) Uses the group PADO delay configuration. • The PADO delay value is sought if the PADO delay is not found after several attempts.
Step 9	**end** **Example:** `Router(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

• Troubleshooting Tips, page 173

Troubleshooting Tips

Use the **debug pppoe event** command to verify the smart server PADO delay selection.

Configuring PPPoE Service PADO Delay

Perform this task to specify a delay based on the PPPoE service. A delay is applied to the PADO offering based on the service name match.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policymap-name*
4. **exit**
5. **bba-group pppoe** [**global** | *profile-name*]
6. **virtual-template** *interface-number*
7. **service profile** *subscriber-profile-name* **refresh** *minutes*
8. **service name match**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.5
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policymap-name* **Example:** `Router(config)# policy-map type service serv3`	Places the router in service policy map configuration mode, and defines the name of service policy map.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits configuration mode and returns to EXEC command mode.

	Command or Action	Purpose
Step 5	**bba-group pppoe** [**global** | *profile-name*] **Example:** `Router(config-bba-group)# bba-group pppoe global`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port.
Step 6	**virtual-template** *interface-number* **Example:** `(config-bba-group)# virtual-template 20`	Specifies the virtual template interface number for the BBA group, and places the router in configuration BBA group mode.
Step 7	**service profile** *subscriber-profile-name* **refresh** *minutes* **Example:** `Router(config-bba-group)# service profile serv3 refresh 30`	Specifies the subscriber profile to be associated with the BBA group, and the refresh interval minutes for the service profile.
Step 8	**service name match** **Example:** `Router(config-bba-group)# service name match`	Matches the requested tag for the PPPoE global group. **Note** The **service name match** command must be configured per the PPPoE service delay. The requested service by the client should also be configured on the BRAS to ensure PADO response from the BRAS.
Step 9	**end** **Example:** `(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

• Troubleshooting Tips, page 175

Troubleshooting Tips

Use the **debug pppoe event**command to verify the service name match and PADO delay for a PPPoE service.

Configuration Examples for PPPoE Smart Server Selection

• Configuring BBA Group PADO Delay Example, page 176
• Configuring PADO Delay Example, page 176
• Configuring PPPoE Service PADO Delay Example, page 176

- Verifying the PPPoE Service Match and PADO Delay Example, page 176

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
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	*Cisco IOS XE Broadband and DSL Configuration Guide*
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* • Cisco IOS Master Command List, All Releases

Standards

Standard	Title
None	-

MIBs

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

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

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

Feature Information for PPPoE Smart Server Selection

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

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

Table 19 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.

Monitoring PPPoE Sessions with SNMP

The PPPoE Session Count Management Information Base feature provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPP over Ethernet (PPPoE) sessions configured on permanent virtual circuits (PVCs) and on a router.

The SNMP Traps for PPPoE Session Limits feature provides SNMP MIB support for the PPPoE session limits and generates notifications in case the limits are reached.

This MIB also supports two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router. The PPPoE session-count thresholds can be configured using the **sessions max limit** and **pppoe max-sessions** commands.

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 Table at the end of this document.

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

Prerequisites for Monitoring PPPoE Sessions with SNMP

- You must understand the concepts described in the Preparing for Broadband Access Aggregation module.
- PPPoE sessions must be established using the procedures in the Providing Protocol Support for Broadband Access Aggregation of PPPoE Session s module.

Restrictions for Monitoring PPPoE Sessions with SNMP

The **snmp-server enable traps pppoe** command enables SNMP traps only. It does not support inform requests.

Information About Monitoring PPPoE Sessions with SNMP

Network Management Protocol

SNMP is a network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security. SNMP version 2 supports centralized and distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

PPPoE Session Count MIB

A MIB is a database of network management information that is used and maintained by a network management protocol, such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system.

The PPPoE Session Count MIB uses two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router. The PPPoE session-count thresholds can be configured using the **sessions max limit** and **pppoe max-sessions** commands. You can also set per-MAC session and IWF limits for a PPPoE session, per-MAC throttle rate limit for a PPPoE session, per-VLAN session configuration limit, per-VLAN throttle rate limit, per-VC session configuration limit, and per-VC throttle rate limit configuration limit.

The table below describes the objects and tables supported by the PPPoE Session-Count MIB. For a complete description of the MIB, see the PPPoE Sessions Management MIB file CISCO-PPPOE-MIB.my, available through Cisco.com at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index.

Table 20 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.

Object or Table	Description
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

Configuring the PPPoE Session-Count Threshold for the Router

Perform this task to configure the PPPoE session-count threshold for the router.

Note The **sessions max limit** command is available only if you configure the **bba-group pppoe** command using the **global** keyword.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **bba-group pppoe** {*group-name* | **global**}
5. **sessions max limit** *session-number* [**threshold** *threshold-value*]
6. **virtual-template** *template-number*
7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE sessions have been reached.

	Command or Action	Purpose
Step 4	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe global`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode.
Step 5	**sessions max limit** *session-number* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions max limit 4000 threshold 3000`	Configures the PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold at which an SNMP trap will be generated. **Note** This command applies only to the global profile.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies the virtual template that will be used to clone the virtual access interfaces (VAI).
Step 7	**end** **Example:** `Router(config-bba-group)# end`	Exits BBA group configuration mode and returns to privileged EXEC mode.
Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a PVC

Perform this task to configure the PPPoE session-count threshold for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **pvc** [*name*] *vpi* / *vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe**
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 5/120`	Creates an ATM PVC and enters ATM VC configuration mode.

	Command or Action	Purpose
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-vc)# pppoe max-sessions 5 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 7	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPPoE sessions to be established on ATM PVCs.
Step 8	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits ATM VC configuration mode and returns to sub interface mode.
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for a VC Class

Perform this task to configure the PPPoE session-count threshold for a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **vc-class atm** *name*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **protocol pppoe** [**group** *group-name* | **global**]
7. **end**
8. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm main`	Creates a VC class for an ATM PVC, or SVC, or ATM interface and enters VC class configuration mode.
Step 5	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-vc-class)# pppoe max-sessions 7 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-vc-class)# protocol pppoe group one`	Enables PPPoE sessions to be established.
Step 7	**end** **Example:** `Router(config-vc-class)# end`	(Optional) Exits VC class configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* **/** *subslot* **/** *port* [*.subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **protocol pppoe** [**group** *group-name* | **global**]
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.

	Command or Action	Purpose
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters the subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 3/100 3/105`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-range)# pppoe max-sessions 20 threshold-sessions 15`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 7	**protocol pppoe** [**group** *group-name* | **global**] **Example:** `Router(config-if-atm-range)# protocol pppoe group two`	Enables PPPoE sessions to be established.
Step 8	**end** **Example:** `Router(config-if-atm-range)# end`	(Optional) Exits ATM PVC range configuration mode and returns to privileged EXEC mode.
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range

Perform this task to configure the PPPoE session-count threshold for an individual PVC within an ATM PVC range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
4. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
5. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci
6. **pvc-in-range** [*pvc-name*] [*vpi* / *vci*]
7. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
8. **end**
9. **more system:running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	(Optional) Enables PPPoE session count SNMP notifications. • This command enables SNMP traps that send notification messages when PPPoE session thresholds have been reached.
Step 4	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode.
Step 5	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci **Example:** `Router(config-subif)# range range1 pvc 3/100 4/199`	Defines a range of ATM PVCs and enters ATM PVC Range configuration mode.

	Command or Action	Purpose
Step 6	**pvc-in-range** [*pvc-name*] [*vpi* / *vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Configures an individual PVC within a PVC range and enters ATM PVC-in-range configuration mode.
Step 7	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(cfg-if-atm-range-pvc)# pppoe max-sessions 10 threshold-sessions 5`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 8	**end** **Example:** `Router(cfg-if-atm-range-pvc)# end`	(Optional) Exits ATM PVC-in-range configuration mode and returns to privileged EXEC mode.
Step 9	**more system:running-config** **Example:** `Router(#) more system:running-config`	Displays the running configuration and the PPPoE session-count thresholds.

Monitoring and Maintaining PPPoE Session Counts and SNMP Notifications

Perform the following task to monitor PPPoE sessions counts and SNMP notifications.

SUMMARY STEPS

1. **enable**
2. **debug snmp packets**
3. **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
4. **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
5. **show vpdn session**
6. **show pppoe session**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password when prompted.

Example:

```
Router> enable
```

Step 2 **debug snmp packets**

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

Example:

```
Router# debug snmp packets
SNMP: Packet received via UDP from 192.0.2.11 on GigabitEthernet1/0
SNMP: Get-next request, reqid 23584, errstat 0, erridx 0
 sysUpTime = NULL TYPE/VALUE
 system.1 = NULL TYPE/VALUE
 system.6 = NULL TYPE/VALUE
SNMP: Response, reqid 23584, errstat 0, erridx 0
 sysUpTime.0 = 2217027
 system.1.0 = Cisco Internetwork Operating System Software
 system.6.0 =
SNMP: Packet sent via UDP to 192.0.2.11
```

Step 3 **debug pppoe errors** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.

Example:

```
Router# debug pppoe errors interface atm 1/0.10
PPPoE protocol errors debugging is on
Router#
00:44:30:PPPoE 0:Max session count(1) on mac(00b0.c2e9.c470) reached.
00:44:30:PPPoE 0:Over limit or Resource low. R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101
ATM1/0.10
```

Step 4 **debug pppoe** events [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

Use this command to display PPPoE protocol messages about events that are part of normal session establishment or shutdown:

Example:

```
Router# debug pppoe events interface atm 1/0.10 vc 101

PPPoE protocol events debugging is on
Router#
00:41:55:PPPoE 0:I PADI  R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101 ATM1/0.10
00:41:55:PPPoE 0:O PADO, R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE 0:I PADR  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:PPPoE :encap string prepared
00:41:55:[3]PPPoE 3:Access IE handle allocated
00:41:55:[3]PPPoE 3:pppoe SSS switch updated
00:41:55:[3]PPPoE 3:AAA unique ID allocated
00:41:55:[3]PPPoE 3:No AAA accounting method list
00:41:55:[3]PPPoE 3:Service request sent to SSS
00:41:55:[3]PPPoE 3:Created  R:0001.c9f0.0c1c L:00b0.c2e9.c470 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State REQ_NASPORT    Event MORE_KEYS
00:41:55:[3]PPPoE 3:O PADS  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM1/0.10
00:41:55:[3]PPPoE 3:State START_PPP    Event DYN_BIND
00:41:55:[3]PPPoE 3:data path set to PPP
```

```
00:41:57:[3]PPPoE 3:State LCP_NEGO    Event PPP_LOCAL
00:41:57:PPPoE 3/SB:Sent vtemplate request on base Vi2
00:41:57:[3]PPPoE 3:State CREATE_VA    Event VA_RESP
00:41:57:[3]PPPoE 3:Vi2.1 interface obtained
00:41:57:[3]PPPoE 3:State PTA_BIND    Event STAT_BIND
00:41:57:[3]PPPoE 3:data path set to Virtual Access
00:41:57:[3]PPPoE 3:Connected PTA
```

Step 5 **show vpdn session**

Use this command to display information about active Level 2 Forwarding (L2F) protocol tunnel and message identifiers on a VPDN:

Example:

```
Router# show vpdn session
%No active L2TP tunnels
%No active L2F tunnels
PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID        RemMAC          LocMAC        Intf    VASt    OIntf    VC
1       0010.7b01.2cd9  0090.ab13.bca8  Vi4     UP      AT6/0   0/10
```

Step 6 **show pppoe session**

Use this command to display information about the currently active PPPoE sessions:

Example:

```
Router# show pppoe session
     3 sessions in LOCALLY_TERMINATED (PTA) State
     3 sessions total

Uniq ID  PPPoE  RemMAC          Port            VT  VA         State
           SID  LocMAC                              VA-st      Type
      1      1  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.1      PTA
                001a.3045.0331  VC: 99/100          UP
      2      2  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.2      PTA
                001a.3045.0331  VC: 99/100          UP
      3      3  0007.b3dc.a41c  ATM0/3/1.100     1  Vi2.3      PTA
                001a.3045.0331  VC: 99/100          UP
Router#
```

Configuration Examples for Monitoring PPPoE Sessions with SNMP

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 pppoe1
 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	Understanding Broadband Access Aggregation
Tasks for preparing for broadband access aggregation	Preparing for Broadband Access Aggregation
Configuring PPPoE sessions	Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Related Topic	Document Title
Establishing PPPoE session limits for sessions on a specific PVC or VLAN configured on an L2TP access concentrator	Establishing PPPoE Session Limits per NAS Port
Using service tags to enable a PPPoE server to offer PPPoE clients a selection of service during call setup	Offering PPPoE Clients a Selection of Services During Call Setup
Enabling an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to a LNS or tunnel switch	Enabling PPPoE Relay Discovery and Service Selection Functionality
Configuring the transfer upstream of the PPPoX session speed value	Configuring Upstream Connection Speed Transfer
Identifying a physical subscriber line for RADIUS communication with a RADIUS server	Identifying the Physical Subscriber Line for RADIUS Access and Accounting
Configuring a Cisco Subscriber Service Switch	Configuring Cisco Subscriber Service Switch Policies

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
PPPoE Session Count MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
None	--

Technical Assistance

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

Feature Information for Monitoring PPPoE Sessions with SNMP

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

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

Table 21 Feature Information for Monitoring PPPoE Sessions with SNMP

Feature Name	Releases	Feature Configuration Information
PPPoE Session Count MIB, SNMP Traps for PPPoE Session Limits	Cisco IOS XE Release 2.5.0 Cisco IOS XE Release 2.6	This feature was introduced on Cisco ASR 1000 Series Aggregation Routers. This feature provides the ability to use SNMP to monitor in real time the number of PPP over Ethernet sessions configured on PVCs and on a router. You can also retrieve information from the MIB. The SNMP Traps for PPPoE Session Limits feature implements SNMP MIB support for the PPPoE session limits and generates notifications in case the limits are reached. The following commands were introduced or modified: **snmp-server enable traps pppoe**

PPPoE on ATM

This feature module describes the PPP over Ethernet (PPPoE) on ATM feature. The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator.

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 Table at the end of this document.

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

Prerequisites for PPPoE on ATM

Before you can configure PPPoE on ATM, you need to specify a virtual template for the PPPoE sessions using the **virtual-template** command.

Restrictions for PPPoE on ATM

- PPPoE is not supported on Frame Relay.

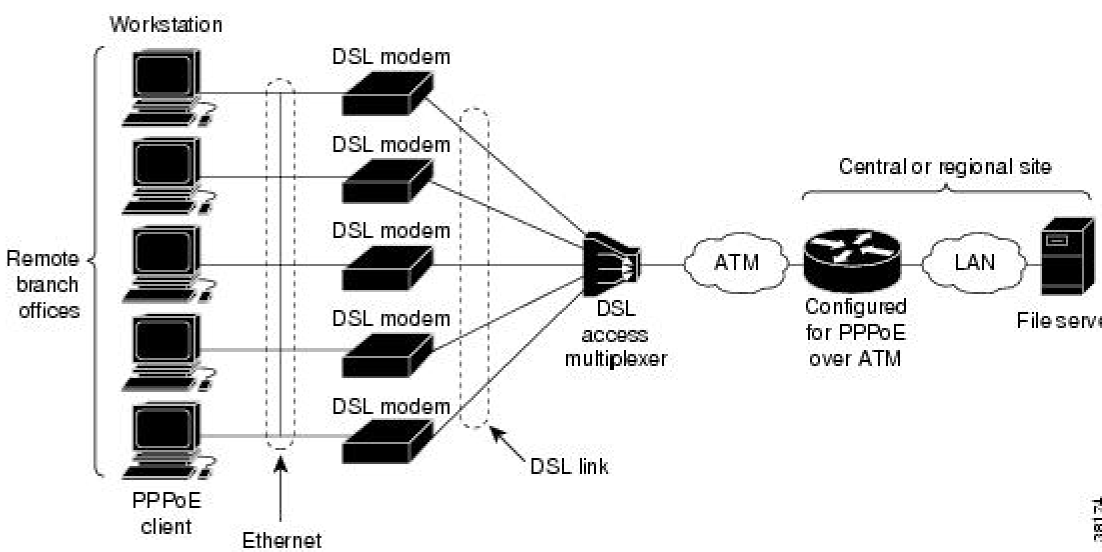
- PPPoE over ATM AAl5Mux is not supported on ASR series 1000 routers. For more information, refer to the PPPoEoA over ATM AAL5Mux feature: http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_pppoeoa_aal5mux.html
- PPPoE is not supported on any other LAN interfaces such as FDDI and Token Ring.
- Fast switching is supported. PPPoE over RFC 1483 fibswitching is supported for IP. All other protocols are switched over process switching.
- Bridging is supported on the ATM permanent virtual connections (PVCs) running PPPoE.
- PPPoE is supported on ATM PVCs compliant with RFC 1483 only.
- Only dial-in mode is supported. Dial-out mode will not be supported.

Information About PPPoE on ATM

The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. With this model, each host utilizes its own PPPoE stack and the user is presented with a familiar user interface. Access control, billing and type of service can be done on a per-user, rather than a per-site, basis. Before a point-to-point connection over Ethernet can be provided, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier. A unique session identifier is provided by the PPPoE Discovery Stage protocol.

The figure below shows a sample network topology using PPPoE on ATM.

Figure 10 PPPoE on ATM Sample Network Topology



- PPPoE Stage Protocols, page 200
- Benefits of PPPoE on ATM, page 201

PPPoE Stage Protocols

PPPoE has two distinct stage protocols. The stage protocols are listed and summarized in the table below.

Table 22 PPPoE Stage Protocols

Stage Protocols	Description
Discovery Stage protocol	Remains stateless until a PPPoE session is established. Once the PPPoE session is established, both the host and the access concentrator *must* allocate the resources for a PPP virtual access interface.
PPP Session Stage protocol	Once the PPPoE session is established, sends PPPoE data as in any other PPP encapsulation.

There are four steps to the Discovery Stage:

1. Host broadcasts a PPPoE Active Discovery Initiation (PADI) packet.
2. When the access concentrator receives a PADI that it can serve, it replies by sending a PPPoE Active Discovery Offer (PADO) packet to the host.
3. Because the PADI was broadcast, the host may receive more than one PADO packet. The host looks through the PADO packets it receives and chooses one. The choice can be based on the AC name or the services offered. The host then sends a single PPPoE Active Discovery Request (PADR) packet to the access concentrator that it has chosen.
4. When the access concentrator receives a PADR packet, it prepares to begin a PPP session. It generates a unique SESSION_ID for the PPPoE session and replies to the host with a PPPoE Active Discovery Session-confirmation (PADS) packet.

When a host wishes to initiate a PPPoE session, it must first perform discovery to identify the Ethernet MAC address of the peer and establish a PPPOE SESSION_ID. Although PPP defines a peer-to-peer relationship, discovery is inherently a client/server relationship. In the discovery process, a host (the client) discovers an access concentrator (the server). Based on the network topology, there may be more than one access concentrator that the host can communicate with. The Discovery Stage allows the host to discover all access concentrators and then select one. When discovery is completed, both the host and the selected access concentrator have the information they will use to build their point-to-point connection over Ethernet.

Benefits of PPPoE on ATM

The PPPoE on ATM feature provides service-provider digital subscriber line (DSL) support. As service providers begin DSL deployments, two of their most significant goals are to ease and facilitate consumer end adoption and to preserve as much of the dialup model as possible. PPPoE serves to advance both of these goals by leveraging ethernet scale curves and embedded base (such as ATM NICs) and by preserving the point-to-point session used by internet service providers (ISPs) in today’s dialup model.

Using a PPPoE client (available from RouterWare), a PPP session can be initiated on an Ethernet connected client through a standard ADSL modem. The session is transported over the ATM DSL link via RFC 1483 Ethernet bridged frames and can terminate either in the LAN emulation client (LEC) central office or the ISP point of presence (POP). The termination device can be an aggregation box such as the Cisco 6400 or a router such as the Cisco 7200 series platforms.

As customers deploy asymmetric DSL (ADSL), they will encounter the need to enable users to access remote-access concentrators via simple bridges connecting Ethernet and ATM networks.

How to Configure PPPoE on ATM

Enabling PPP over ATM

After you configure the Cisco router or access server for Ethernet encapsulation, you must configure the physical interface with the PVC and apply a virtual template with PPP encapsulation to the PVC that it applies to. To configure the physical interface that will carry the PPPoE session and link it to the appropriate virtual template interface, use the following commands:

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
6. **sessions per-mac limit** *per-mac-limit*
7. **exit**
8. **interface atm** *slot / subslot* / *port* [.*subinterface*][**point-to-point** | **multipoint**]
9. **ip address** *ip-address mask* [**secondary**]
10. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
11. **dbs enable** [**aggregated** | **maximum**]
12. Do one of the following:
    - **protocol pppoe group** {*group-name* | **global**}
    - or
    - **encapsulation aal5snap**
13. **create on-demand**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe pppoe-group`	Defines a PPPoE profile, and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 5	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `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. **Note** This command applies only to the global profile.
Step 6	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 4000`	Sets the maximum number of PPPoE sessions permitted per MAC address in a PPPoE profile.
Step 7	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**interface atm** *slot / subslot* / *port* [.*subinterface*][**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 1/0.1 multipoint`	Specifies the ATM interface and enters subinterface configuration mode.
Step 9	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 192.0.10.2 255.255.255.0 secondary`	Sets a primary or secondary IP address for an interface.
Step 10	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-if)# range pvc 101/304 200/400`	Defines a range of ATM permanent virtual circuits (PVCs) and enters ATM range configuration mode.
Step 11	**dbs enable** [**aggregated** | **maximum**] **Example:** `Router(config-if-atm-range)# dbs enable`	Applies the Dynamic Subscriber Bandwidth Selection (DBS) QoS parameters.

	Command or Action	Purpose

Step 12	Do one of the following:
	• **protocol pppoe group** {*group-name* | **global**}
	• or
	• **encapsulation aal5snap**
	
	Example:
	`Router(config-if-atm-range-pvc)# protocol pppoe group two`
	
	Example:
	
	Example:
	
	Example:
	`Router(config-if-atm-range-pvc)# encapsulation aal5snap`
		Enables PPPoE sessions to be established on a PVC within a range.
		or
		Configures PPPoE autosense.
		• If a PPPoE profile is not assigned to the PVC by using the **group** *group-name* option, the PVC will use the global PPPoE profile.

Step 13	**create on-demand** **Example:** `Router(config-if-atm-range)# create on-demand`	Configures ATM PVC autoprovisioning, which enables a range of PVCs to be created automatically on demand.
Step 14	**end** **Example:** `Router(config-if-atm-range)# end`	(Optional) Exits the ATM range configuration mode and returns to privileged EXEC mode.

Creating and Configuring a Virtual Template

Creating and Configuring a Virtual Template

Prior to configuring the ATM PVC for PPPoE on ATM, you typically create and configure a virtual template.

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

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 or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 2`	Creates a virtual template, and enters interface configuration mode.
Step 4	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP encapsulation on the virtual template.
Step 5	**ip unnumbered gigabitethernet** slot/subslot/port[.subinterface] **Example:** `Router(config-if)# ip unnumbered gigabitethernet0/0/0`	Optionally, enables IP without assigning a specific IP address on the LAN.
Step 6	**end** **Example:** `Router(config-if)# end`	(Optional) Exits the interface configuration mode and returns to privileged EXEC mode.

Specifying an ATM Subinterface

After you create a virtual template for PPPoE on ATM, specify a multipoint or point-to-point subinterface per PVC connection. To specify an ATM multipoint subinterface, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* *.subinterface*] [**multipoint**| **point-to-point**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* *.subinterface*] [**multipoint**| **point-to-point**] **Example:** `Router# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode. • A **multipoint** subinterface is recommended for interface conservation. A **point-to-point** subinterface will greatly restrict the total number of PPPoE sessions you can have.
Step 4	**end** **Example:** `Router(config-subif)# end`	(Optional) Exits the subinterface configuration mode and returns to privileged EXEC mode.

Creating an ATM PVC

Creating an ATM PVC

After you create a virtual template and specify an ATM subinterface, you must create an ATM PVC.

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.

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*] v*pi* / *vci*
5. **encapsulation aal5snap**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 6/0.110 multipoint`	Configures the ATM interface and enters subinterface configuration mode.

	Command or Action	Purpose

Step 4	**pvc** [*name*] v*pi* / *vci*
	
	Example:
	
	`Router(config-subif)#`
	` pvc 5/120`
		Creates an ATM PVC and enters ATM VC configuration mode.

Step 5	**encapsulation aal5snap** **Example:** `Router(config-if-atm-vc)# encapsulation aal5snap`	Specifies AAL5 SNAP for ATM encapsulation.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits the ATM VC configuration mode and returns to privileged EXEC mode.

Enabling PPPoE on an ATM PVC

To enable PPPoE on an ATM PVC, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**]
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **protocol pppoe**
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *subslot* / *port* [.*subinterface*] [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface atm 0/0/0.3 multipoint`	Configures the ATM interface and enters the subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 5/120`	Creates an ATM PVC and enters ATM VC configuration mode.
Step 5	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-vc)# pppoe max-sessions 5 threshold-sessions 3`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Enables PPPoE sessions to be established on ATM PVCs.
Step 7	**end** **Example:** `Router(config-if-atm-vc)# end`	(Optional) Exits the ATM VC configuration mode and returns to privileged EXEC mode.

Configuration Examples for PPPoE on ATM

- PPPoE on ATM Example, page 212

PPPoE on ATM Example

The following example configures PPPoE on ATM to accept dial-in PPPoE sessions. The virtual access interface for the PPP session is cloned form virtual template interface 1. On subinterface ATM 2/0.1, ATM PVC with VPI 0 and VCI 60 is configured with Logical Link Control (LLC)/Subnetwork Access Protocol (SNAP) encapsulation and is configured to run PPPoE.

```
bba-group pppoe pppoe-group
 virtual-template 1
 sessions per-vc limit 1
 sessions per-mac limit 4000
interface atm 2/0.1 multipoint
 ip address 192.0.10.2 255.255.255.0 secondary
 range pvc 1/100 1/202
 pvc 0/60
  dbs enable
  encapsulation aal5snap
  protocol pppoe group two
  create on-demand
interface virtual-template 1
  ip addr 10.0.1.2 255.255.255.0
  mtu 1492
```

Where to Go Next

- If you want to enable PPP authentication on the virtual template using the **ppp authentication chap** command, refer to the "Configuring Virtual Template Interfaces" chapter in the *Cisco IOS Dial Solutions Configuration Guide* .
- If you want to configure an authentication, authorization, and accounting (AAA) server, refer to the "Configuring per-User Configuration" chapter in the *Cisco IOS Dial Solutions Configuration Guide* .

Additional References

The following sections provide references related to the PPPoE on ATM feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Broadband and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Enabling PPP authentication on the virtual template	Configuring Virtual Template Interfaces
Configuring an AAA server	Configuring per-User Configuration
Configuring Broadband and DSL	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 1483	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*
RFC 2364	*PPP over AAL5*
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*

Technical Assistance

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

Feature Information for PPPoE on ATM

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

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

Table 23 Feature Information for PPPoE on ATM

Feature Name	Releases	Feature Information
PPPoE on ATM	Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. This feature module describes the PPP over Ethernet (PPPoE) on ATM feature. The PPPoE on ATM feature provides the ability to connect a network of hosts over a simple bridging-access device to a remote access concentrator. The following commands were introduced or modified: **bba-group, protocol (VPDN)**, **virtual-template**.

Glossary

AAL5 --ATM Adaptation Layer 5

ADSL --Asymmetric Digital Subscriber Line

ATM --Asynchronous Transfer Mode

CPCS --Common Part of Convergence Sublayer

CPI --Common Part Indicator

CRC --Cyclic Redundancy Check

DSLAM --Digital Subscriber Line Access Multiplexer

FCS --Frame Check Sequence

IETF --Internet Engineering Task Force

ID -Identifier

IP --Internet Protocol

L2TP --Layer two Tunneling Protocol

LAN --Local Area Network

LLC --Logical Link Control

MAC --Media Access Control

PDU --Protocol Data Unit

PPP --Point to Point Protocol

PPPoE --Point to Point Protocol over Ethernet

PVC --Permanent Virtual Connection

VPDN --Virtual Private Dialup Network

PPPoE on Ethernet

The PPPoE on Ethernet feature adds support to Point-to-Point Protocol over Ethernet (PPPoE) by adding direct connection to actual Ethernet interfaces. PPPoE provides service-provider digital subscriber line (DSL) support. This Ethernet specification can be used by multiple hosts on a shared Ethernet interface to open PPP sessions to multiple destination with one or more bridging modems.

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 Table at the end of this document.

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

Prerequisites for PPPoE on Ethernet

Before you can configure the PPPoE on Ethernet feature, you need to configure a virtual private dialup network (VPDN) group using the **accept dialin** command, enable PPPoE, and specify a virtual template for PPPoE sessions.

Restrictions for PPPoE on Ethernet

- PPPoE is not supported on Frame Relay.
- PPPoE is not supported on any other LAN interfaces such as FDDI and Token Ring.

- Fast switching is supported. PPP over Ethernet over RFC 1483 fibswitching is supported for IP. All other protocols are switched over process switching.

Information About PPPoE on Ethernet

Benefits of Using PPPoE on Ethernet

Broadband Remote Access

For a bridged-Ethernet topology, the PPPoE on Ethernet feature allows access providers to maintain session abstraction associated with PPP networks.

PPPoE

PPPoE provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator where each host utilizes its own PPP stack. It also gives users a familiar interface.

PPPoE provides service-provider DSL support. In service-provider DSL deployments, PPPoE leverages Ethernet scale curves and it uses an embedded base.

How to Enable and Configure PPPoE on Ethernet

Enabling PPPoE on Ethernet in a VPDN Group

To configure the physical interface that will carry the PPPoE session and link it to the appropriate virtual template interface, you need to complete the following steps.

SUMMARY STEPS

1. Router(config)# **vpdn enable**
2. Router(config-if)# **vpdn group** *name*
3. Router(config-if)# **accept dialin**
4. Router(config-if)# **protocol pppoe**
5. Router(config-if)# **virtual-template** *template-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **vpdn enable**	Enables virtual private dial-up networking.
Step 2	Router(config-if)# **vpdn group** *name*	Associates a VPDN group to a customer or VPDN profile.
Step 3	Router(config-if)# **accept dialin**	Creates an accept dial-in VPDN group.
Step 4	Router(config-if)# **protocol pppoe**	Specifies the VPDN group to be used to establish PPPoE sessions.
Step 5	Router(config-if)# **virtual-template** *template-number*	Specifies which virtual template will be used to clone virtual access interfaces.

Limiting PPPoE Sessions from a MAC Address

To set the limit of sessions to be sourced from a MAC address, use the following command in VPDN configuration mode:

Command	Purpose
`Router(config-if)#` **`pppoe session-limit per-mac`** `number`	Sets the limit of sessions to be sourced from a MAC address.

Creating and Configuring a Virtual Template

Other optional configuration commands can be added to the virtual template configuration. For example, you can enable the PPP authentication on the virtual template using the **ppp authentication chap** command. See the " Virtual Interface Template Service " chapter in the *Cisco IOS Dial S>olutions Configuration Guide* for more information about configuring the virtual template.

Although Cisco Express Forwarding switching is supported, flow, and optimum switching are not; these configurations are ignored on the PPPoE virtual access interface. Cisco Express Forwarding is enabled by default for IP. All other protocol traffic will be processed switched.

Note The PPP reliable link that uses Link Access Procedure, Balanced (LAPB) is not supported.

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

SUMMARY STEPS

1. Router(config)# **interface virtual-template** *number*
2. Router(config-if)# **ip unnumbered ethernet** *number*
3. Router(config-if)# **mtu** *bytes*

DETAILED STEPS

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

Specifying an Ethernet Interface

After you create a virtual template for PPPoE on Ethernet, specify a multipoint or point-to-point interface. To specify an Ethernet multipoint interface, use the following commands in global configuration mode:

Command	Purpose
`Router#` **`interface ethernet`** `interface-number`	Specifies the Ethernet interface using the appropriate format of the **interface ethernet** command.

Enabling PPPoE on an Ethernet Interface

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

Command	Purpose
`Router#` **`pppoe enable`**	Specifies the VPDN group to be used for establishing PPPoE sessions.

Monitoring and Maintaining VPDN Groups

To monitor and maintain VPDN groups, use the following commands in EXEC mode:

Command	Purpose
`Router#` **show vpdn**	Displays information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN.
`Router#` **show vpdn session packet**	Displays PPPoE session statistics.
`Router#` **show vpdn session all**	Displays PPPoE session information for each session ID.
`Router#` **show vpdn tunnel**	Displays PPPoE session count for the tunnel.

Configuration Examples for PPPoE on Ethernet

PPPoE on Ethernet Example

The following are examples of the **vpdn enable** and **interface virtual-template** commands:

```
vpdn enable

 vpdn-group 1
 accept dialin
 protocol pppoe
 virtual template 1
 pppoe limit per-mac <number>

 interface virtual-template 1
 ip address 10.100.100.100 255.255.255.0
 mtu 1492
```

For PPPoE virtual template interfaces, the **mtu** command must be configured because Ethernet has a maximum payload size of 1500 bytes, the PPPoE header is 6 bytes, and PPP Protocol ID is 2 bytes.

Note Dial-out mode will not be supported.

Enabling PPPoE on an Ethernet Interface Example

The following example enables PPPoE on an Ethernet interface:

```
interface ethernet1/0
 pppoe enable
```

Additional References

The following sections provide references related to the PPPoE on Ethernet feature.

Related Documents

Related Topic	Document Title
Configuring PPPoE on ATM	PPPoE over ATM
Configuring PPPoE on cable interfaces	• Point-to-Point Protocol over Ethernet Support on the Cisco CMTS • Configuring PPPoE Termination on a uBR7100 CMTS with L2TP Tunneling
Configuring PPPoE on IEEE 802.1Q encapsulation	PPPoE Over IEEE 802.1Q VLANs

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPPoE*
RFC 4813	Multiprotocol Encapsulation over ATM Adaptation Layer 5

Technical Assistance

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

Feature Information for PPPoE on Ethernet

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

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

Table 24 Feature Information for PPPoE on Ethernet

Feature Name	Releases	Feature Information
PPPoE on Ethernet	Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The PPPoE on Ethernet feature adds support to Point-to-Point Protocol over Ethernet (PPPoE) by adding direct connection to actual Ethernet interfaces. PPPoE provides service-provider digital subscriber line (DSL) support. This Ethernet specification can be used by multiple hosts on a shared Ethernet interface to open PPP sessions to multiple destination with one or more bridging modems.

Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end Virtual Private Network (VPN) service to remote users. This feature integrates the Multiprotocol Label Switching (MPLS)-enabled backbone with broadband access capabilities.

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 Table at the end of this document.

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

Prerequisites for Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature has the following prerequisites:

- Your network must be running the following Cisco IOS XE services before you configure VPN operation:
  - MPLS in the service provider backbone routers
  - Tag Distribution Protocol (TDP) or the Label Distribution Protocol (LDP)
  - Border Gateway Protocol (BGP) in all routers providing a VPN service
  - Cisco Express Forwarding switching in each MPLS-enabled router
- The provider edge (PE) routers that belong to the same VPN must be configured with the same VPN ID. The VPN ID must be unique to the service provider network.

Restrictions for Remote Access MPLS-VPNs

The Remote Access MPLS-VPNs feature has the following restrictions:

- The VPN ID is not used to control the distribution of routing information or to associate IP addresses.

Information About Remote Access MPLS-VPNs

Introduction to Remote Access MPLS-VPNs

MPLS-based VPNs allow service providers to deploy a scalable and cost-effective VPN service that provides a stable and secure path through the network. An enterprise connects to geographically dispersed sites in the Internet service provider's (ISPs) network through use of an MPLS backbone. Sites are interconnected to create an MPLS VPN.

The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. The Remote Access MPLS-VPNs feature integrates the MPLS-enabled backbone with broadband access capabilities. By integrating access VPNs with MPLS VPNs, a service provider can:

- Enable remote users and offices to seamlessly access their corporate networks
- Offer equal access to a set of different ISPs or retail service providers
- Integrate their broadband access networks with the MPLS-enabled backbone
- Provide end-to-end VPN service to enterprise customers with remote access (RA) users and offices
- Separate network access and connectivity functions from ISP functions

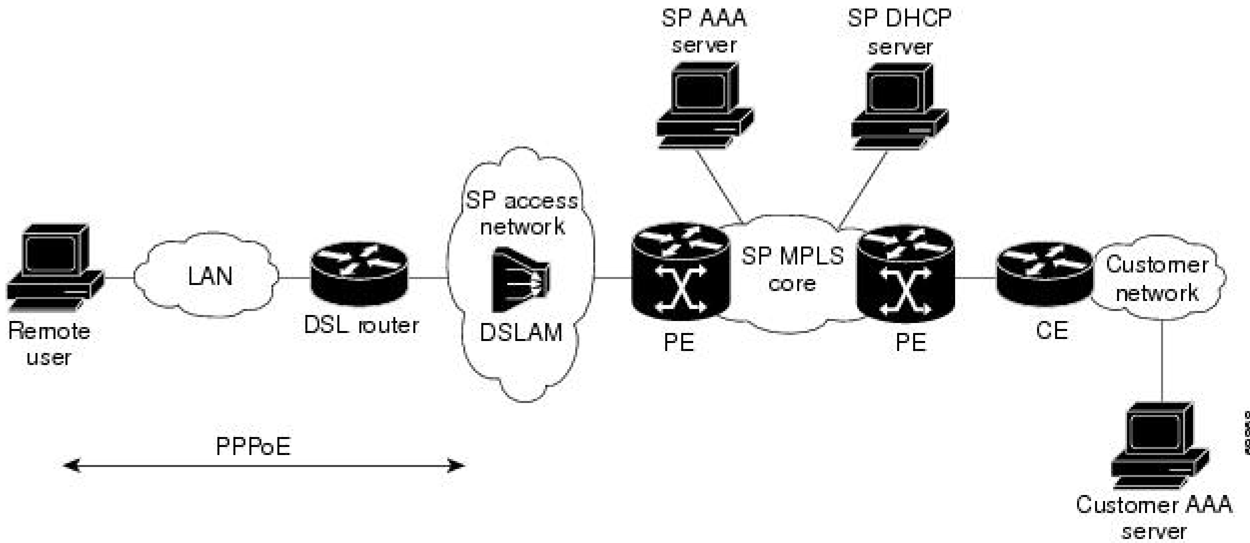
MPLS VPN Architecture

MPLS VPN architecture enables the service provider to build the MPLS VPN network one time and add VPNs for new customers as needed, including them in the already established network. The elements that comprise the MPLS VPN are:

- Customer edge (CE) routers--The routers to which subscribers in a customer's network connect. The CE router connects to a service provider's edge router (PE router). The CE router initiates the remote access session to the PE router.
- Provider edge (PE) routers--The routers located at the edge of the service provider's MPLS core network. The PE router connects to one or more CE routers and has full knowledge of the routes to the VPNs associated with those CE routers. The PE router does not have knowledge of the routes to VPNs whose associated CE routers are not connected to it.
- Provider (P) routers--The service provider routers that comprise the provider's core network. The P routers do not assign VPN information and they do not have any knowledge of CE routers. Instead, the main focus of the P router is on label switching.

The figure below shows an example of MPLS VPN network architecture.

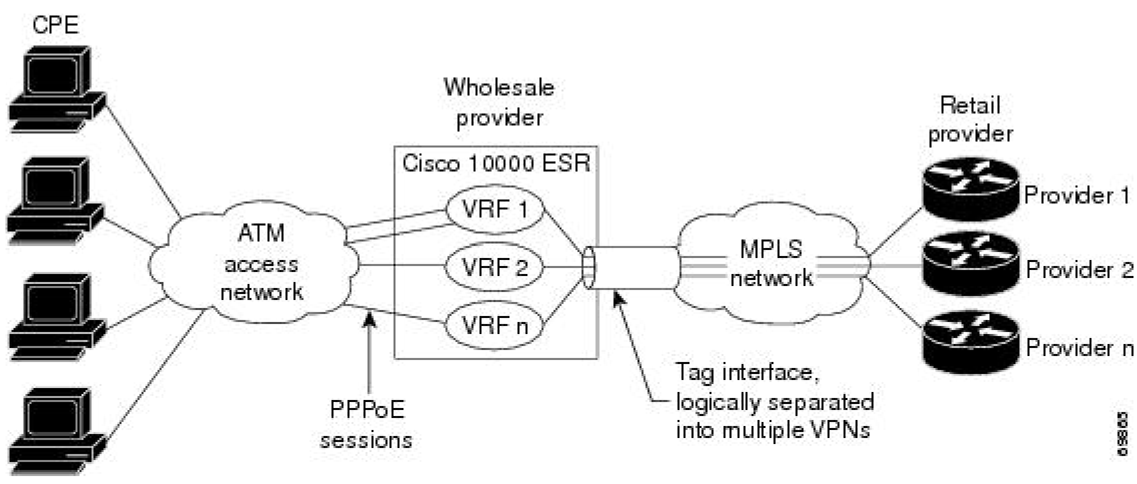
Figure 11 MPLS VPN Network--Example



PPP over Ethernet to MPLS VPN

The figure below shows the topology of integrated PPP over Ethernet (PPPoE) access to an MPLS VPN.

Figure 12 PPPoE Access to MPLS VPN Topology



In the figure above, the service provider operates an MPLS VPN that interconnects all customer sites. The service provider's core network is an MPLS backbone with VPN service capability. The service provider provides all remote access operations to its customer. The network-side interfaces are tagged interfaces, logically separated into multiple VPNs.

Remote access is provided using a PPPoE connection. In this model, when a remote user attempts to establish a connection with a corporate network, a PPPoE session is initiated and is terminated on the service provider's virtual home gateway (VHG) or PE router. All remote hosts connected to a particular CE router must be part of the VPN to which the CE router is connected.

The PPPoE to MPLS VPN architecture is a flexible architecture with the following characteristics:

- A remote host can create multiple concurrent PPPoE sessions, each to a different VPN.
- If multiple remote hosts exist behind the same CE router, each remote host can log in to a different VPN.
- Any remote host can log in to any VPN at any time because each VHG or PE router has the VRFs for all possible VPNs preinstantiated on it. This configuration requires that the VRF be applied through the RADIUS server, which can cause scalability issues.

The following events occur as the VHG or PE router processes the incoming PPPoE session:

1. A PPPoE session is initiated over the broadband access network.
2. The VHG/PE router accepts and terminates the PPPoE session.
3. The VHG/PE router obtains virtual access interface (VAI) configuration information:
    - The VHG/PE obtains a virtual template interface configuration information, which typically includes VRF mapping for sessions.
    - The VHG/PE sends a separate request to either the customer's or service provider's RADIUS server for the VPN to authenticate the remote user.
    - The VPN's VRF instance is instantiated on the VHG or PE. The VPN's VRF contains a routing table and other information associated with a specific VPN.

Typically, the customer RADIUS server is located within the customer VPN. To ensure that transactions between the VHG/PE router and the customer RADIUS server occur over routes within the customer VPN, the VHG/PE router is assigned at least one IP address that is valid within the VPN.

1. The VHG/PE router forwards accounting records to the service provider's proxy RADIUS server, which in turn logs the accounting records and forwards them to the appropriate customer RADIUS server.
2. The VHG/PE obtains an IP address for the CPE. The address is allocated from one of the following:
    - Local address pool
    - Service provider's RADIUS server, which either specifies the address pool or directly provides the address
    - Service provider's DHCP server
3. The CPE is now connected to the customer VPN. Packets can flow to and from the remote user.

How to Configure Remote Access MPLS-VPNs

- Configuring the MPLS Core Network, page 228
- Configuring PPPoE, page 229
- Configuring and Associating Virtual Private Networks, page 232

Configuring the MPLS Core Network

The MPLS core network is configured by enabling label switching of IP packets on interfaces, configuring virtual routing and forwarding instances, associating VRFs and configuring Multiprotocol BGP PE-to-PE routing sessions. For details relating to these activities, see the appropriate section of the *Cisco IOS XE Multiprotocol Label Switching Configuration Guide.*

Configuring PPPoE

Configuring a Virtual Template Interface

To create and configure a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, perform the steps in the following task.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**ip unnumbered ethernet** *number* **Example:** `Router(config-if)# ip unnumbered ethernet 1`	Enables IP without assigning a specific IP address on the LAN.

	Command or Action	Purpose
Step 5	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 6	**ppp ipcp address required** **Example:** `Router(config-if)# ppp ipcp address required`	(Required for legacy dialup and DSL networks.) Prevents a PPP session from being configured with 0.0.0.0 remote ip address.

Configuring PPPoE in a Broadband Aggregation Group

To configure a broadband aggregation (BBA) group for PPPoE and to link it to the appropriate virtual template interface, perform the steps in the following task.

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 max limit** *global-pppoe-session-limit*
7. **exit**
8. **interface gigabitethernet** *slot/subslot/port.* [*subinterface*]
9. Command or Action
10. **encapsulation dot1q** *vlan-id*
11. **pppoe enable** [**group** *group-name*]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {**name** | **global**} **Example:** `Router(config)# bba-group pppoe bba1`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA configuration mode • The name argument identifies the BBA group. You can have multiple BBA groups. • The global keyword is the default BBA group used when a BBA group name is not specified.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba)# virtual-template 20`	Specifies the virtual template interface to use to clone virtual access interfaces (VAIs).
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba)# sessions per-mac limit 32000`	(Optional) Specifies the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile.
Step 6	**sessions max limit** *global-pppoe-session-limit* **Example:** `Router(config-bba)# sessions max limit 32000`	(Optional) Specifies the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold
Step 7	**exit** **Example:** `Router(config-bba)# exit`	Returns to global configuration mode.
Step 8	**interface gigabitethernet** *slot/subslot/port.* [*subinterface*] **Example:** `Router(config)# interface gigabitethernet 2/0/0.2`	Specifies the interface to which you want to attach the BBA group.
Step 9	Command or Action	Purpose

	Command or Action	Purpose
Step 10	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 2`	Creates an 802.1q sub-interface and specifies the VLAN id.
Step 11	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-subif)# pppoe enable group bba1`	Attaches the BBA group to the VLAN.

Configuring and Associating Virtual Private Networks

A Virtual Private Network (VPN) service can be added to your MPLS configuration by configuring VPNs and associating the VPNs with a virtual template interface. For details relating to these activities, see the Configuring MPLS Layer 3 VPNs module.

Configuration Examples for Remote Access MPLS-VPNs

Example Configuring Remote Access MPLS-VPNs with One VRF for PPPoE Sessions

The following example shows how to configure the RA to MPLS VPN feature with one VRF for PPPoE sessions:

```
!
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default local
aaa session-id common
enable password cisco
!
username pppoe password 0 pppoe
username common password 0 common
!
!Creates the common VRF.
ip vrf common
rd 100:1000
route-target export 100:1000
route-target import 100:1000
!
```

```
!Specifies the BBA group to be used to establish PPPoE sessions and specifies the maximum
!number of PPPoE sessions to be established over a vlan.
bba-group pppoe
virtual-template 1
sessions per-mac limit 32000
!
no virtual-template snmp
!
!Configures the small buffer.
buffers small permanent 15000
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
ip address 10.16.3.1 255.255.255.255
ip ospf network point-to-point
!
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP
!unnumber interfaces to.
interface Loopback1
ip vrf forwarding vpn1
ip address 10.24.1.1 255.255.255.255
!
interface Loopback2
ip vrf forwarding vpn2
ip address 10.8.1.2 255.255.255.255
!
interface gigaethernet 0/0/0
load-interval 30
negotiation auto
no cdp enable
interface gigaethernet 0/0/0.9
encapsulation dot1q 9
pppoe enable
no cdp enable
!
!Enables label switching of IP packets on the interface.
interface GigabitEthernet1/0/0
ip address 10.1.10.1 255.255.0.0
no ip redirects
load-interval 30
negotiation auto
tag-switching ip
!
!Defines the virtual template and associates the common VRF with it.
interface Virtual-Template1
ip vrf forwarding common
ip unnumbered Loopback1
peer default ip address pool common
ppp authentication chap
!
!Configures OSPF to advertise the networks.
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 10.16.3.1 0.0.0.0 area 0
network 10.1.0.0 0.0.255.255 area 0
!
router rip
version 2
!
!Enters address family configuration mode to configure the VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
version 2
network 10.0.0.0
no auto-summary
exit-address-family
!
!Configures BGP to advertise the networks for the VPN.
router bgp 100
no synchronization
no bgp default ipv4-unicast
```

```
bgp log-neighbor-changes
neighbor 172.16.1.4 remote-as 100
neighbor 172.16.1.4 activate
!
!Enters address family configuration mode to configure the common VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
no auto-summary
no synchronization
aggregate-address 10.10.0.0 255.255.0.0 summary-only
exit-address-family
!
address-family vpnv4
neighbor 172.16.1.4 activate
neighbor 172.16.1.4 send-community both
exit-address-family
!
!Specifies the IP local pool to use for the VRF address assignment.
ip local pool common 10.10.1.1 10.10.126.0
ip classless
!Enters routing information in the routing table for the VRF.
ip route 10.0.0.0 255.0.0.0 FastEthernet0/0/0 10.9.0.1
ip route vrf common 10.22.0.0 255.255.0.0 Null0
ip route vrf common 10.30.0.0 255.255.0.0 2.1.1.1 3
ip route vrf common 10.32.0.0 255.255.0.0 2.2.151.1 2
ip route vrf common 10.33.0.0 255.255.0.0 2.3.101.1 2
no ip http server
ip pim bidir-enable
!
no cdp run
!
!Specifies the RADIUS host and configures RADIUS accounting. radius-server retransmit is
!on by default and cannot be removed.
radius-server host 10.19.100.150 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key test
radius-server authorization permit missing Service-Type
radius-server vsa send authentication
call admission limit 90
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Description of commands associated with MPLS and MPLS applications	*Cisco IOS Multiprotocol Label Switching Command Reference*
Basic MPLS VPNs	Configuring MPLS Layer 3 VPNs

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Remote Access MPLS-VPNs

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

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

Table 25 Feature Information for Remote Access MPLS-VPNs

Feature Name	Releases	Feature Information
Remote Access MPLS-VPNs	Cisco IOS XE Release 2.1	The Remote Access MPLS-VPNs feature allows the service provider to offer a scalable end-to-end VPN service to remote users. This feature integrates the MPLS-enabled backbone with broadband access capabilities. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Glossary

CE --customer edge.

PPPoE --Point-to-Point Protocol over Ethernet.

PE --provider edge.

Broadband High Availability Stateful Switchover

The Cisco IOS XE Broadband High Availability Stateful Switchover feature provides the capability for dual Route Processor systems to support stateful switchover of Point-to-Point Protocol over X (PPPoX, where X designates a family of encapsulating communications protocols such as PPP over Ethernet [PPPoE], PPP over ATM [PPPoA], PPPoEoA, PPPoEoVLAN implementing PPP) sessions, thus allowing applications and features to maintain a stateful state while system control and routing protocol execution is transferred between an active and a standby processor.

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 Table at the end of this document.

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

Prerequisites for Broadband High Availability Stateful Switchover

The stateful switchover (SSO) and nonstop forwarding (NSF) features must be enabled. For more information about SSO, see the "Stateful Switchover" module. For more information about NSF, see the "Configuring Nonstop Forwarding" module.

Restrictions for Broadband High Availability Stateful Switchover

SSO is supported only on High Availability (HA) network devices.

Information About Broadband High Availability Stateful Switchover

Feature Design of Broadband High Availability Stateful Switchover

Prior to the implementation of the Broadband High Availability Stateful Switchover feature, unplanned control plane and dataplane failures resulted in service outages and network downtime for PPPoX sessions. Cisco HA features, including SSO, enable network protection by providing fast recovery from such failures. The Broadband High Availability Stateful Switchover feature eliminates a source of outages by providing for stateful switchover to a standby processor while continuing to forward traffic. SSO protects from hardware or software faults on an active Route Processor (RP) by synchronizing protocol and state information for supported features with a standby RP, ensuring no interruption of sessions or connections if a switchover occurs.

The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active processor, designating the other RP as the standby processor, and then synchronizing critical state information between them. Following an initial (bulk) synchronization between the two processors, SSO dynamically maintains RP state information between them. A switchover from the active to the standby processor occurs when the active RP fails, when it is removed from the networking device, or when it is manually taken down for maintenance. The standby RP then takes control and becomes the active RP, preserving the sessions and connections for the supported features. At this time, packet forwarding continues while route convergence is completed on the newly active RP. A critical component of SSO and Cisco HA technology is the cluster control manager (CCM) that manages session re-creation on the standby processor. The Broadband High Availability Stateful Switchover feature allows you to configure subscriber redundancy policies that tune the synchronization process. For more information, see the Configuring Subscriber Redundancy Policy for Broadband HA Stateful Switchover, page 241.

The Broadband High Availability Stateful Switchover feature works with the Cisco NSF and SSO HA features, to maintain PPPoX sessions. NSF forwards network traffic and application state information so that user session information is maintained after a switchover.

For information about High Availability and stateful switchover, see the "High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide .

Supported Broadband Aggregation Protocols

The Broadband High Availability Stateful Switchover feature set supports the broadband aggregation protocols described in the following sections:

SSO PPPoA

The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over ATM (PPPoA) sessions during Route Processor switchover.

SSO L2TP

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic stateful switchover/In Service Software Upgrade (SSO/ISSU) mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

SSO PPPoE

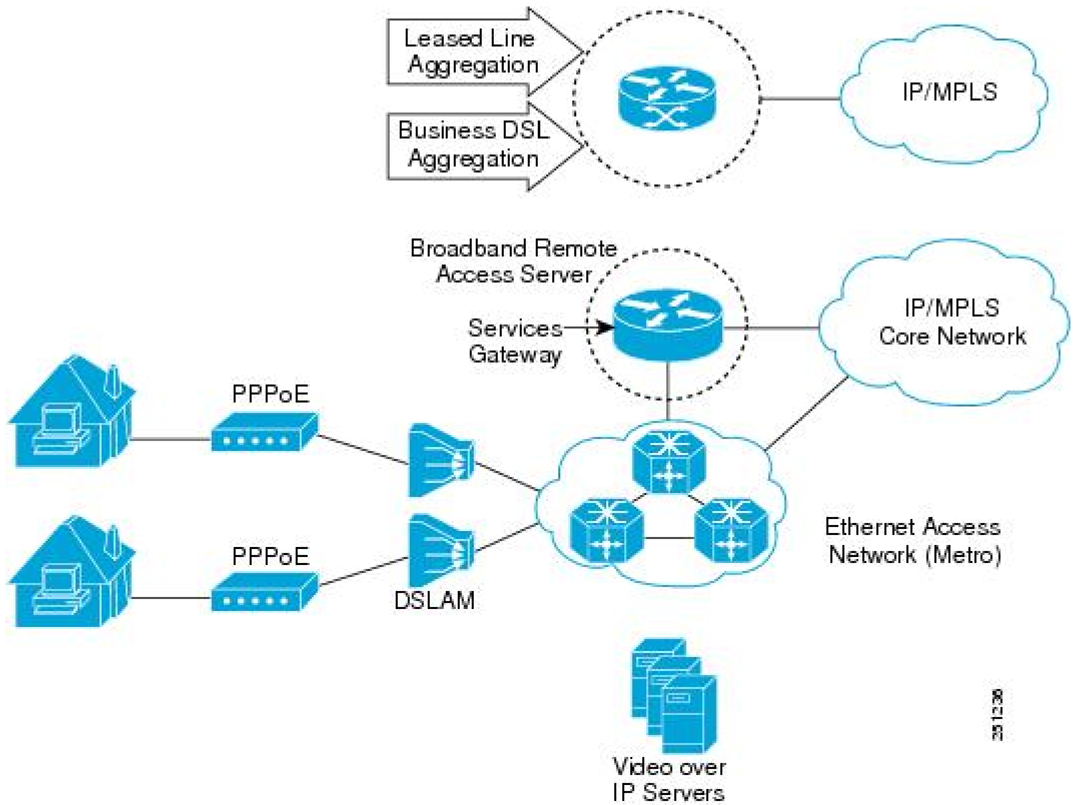
The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoEoVLAN, and PPPoEoQinQ.

SSO RA-MLPS VPN

The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPPoX terminated into remote access (RA)-Multiprotocol Label Switching (MPLS) VPN or PPPoX into MPLS VPN sessions during processor switchover.

The figure below shows a typical broadband aggregation HA deployment with SSO functionality.

Figure 13 Broadband Aggregation High Availability Deployment



Benefits of Broadband High Availability Stateful Switchover

- Reduces operating costs associated with outages.
- Delivers higher service levels to subscribers.
- Improves network availability.
- Promotes continuous connectivity, lower packet loss, and consistent path flow through nodes providing specific network services.
- Mitigates service disruptions, reduces downtime costs, and increases operational efficiency.

How to Configure Broadband High Availability Stateful Switchover

Configuring Subscriber Redundancy Policy for Broadband HA Stateful Switchover

Perform this task to configure subscriber redundancy policy for HA SSO capability for broadband subscriber sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy { bulk limit { cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | time** *seconds* **} | dynamic limit cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | delay** *seconds* **| rate** *sessions seconds* **}**
4. **exit**

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	**subscriber redundancy { bulk limit { cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | time** *seconds* **} | dynamic limit cpu** *percent* **delay** *seconds* **[allow** *sessions* **] | delay** *seconds* **| rate** *sessions seconds* **}**
	
	Example:
	
	`Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`
		(Optional) Configures subscriber redundancy policy.
		• **bulk** --Configures bulk synchronization redundancy policy.
		• **limit** --Specifies the limit for the synchronization.
		• **cpu** *percent* --Specifies a CPU busy threshold value as a percentage. Range is from 0 to 100; default is 90.
		• **delay** *seconds* --Specifies the minimum amount of time, in seconds, that a session must be ready before bulk or dynamic synchronization occurs. Range is from 1 to 33550.
		• **allow** *sessions* --(Optional) Specifies the minimum number of sessions to synchronize once the CPU busy threshold is exceeded and the specified delay is met. Range is from 1 to 2147483637; default is 25.
		• **dynamic** --Configures a dynamic synchronization redundancy policy.
		• **rate** *sessions seconds* --Specifies the number of sessions per time period for bulk and dynamic synchronization.
		    ◦ *sessions*--Range is from 1 to 32000; default is 250.
		    ◦ *seconds*--Range in seconds is from 1 to 33550; default is 1.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA Stateful Switchover

To view the configuration, use the **show running-config** command. Sample output is available at Configuration Examples for Broadband High Availability Stateful Switchover, page 248.

SUMMARY STEPS

1. **show ccm clients**
2. show ccm sessions
3. show ppp subscriber statistics
4. **show pppatm statistics**
5. **show pppoe statistics**
6. **show vpdn redundancy**
7. **show vpdn history failure**
8. **show pppatm redundancy**
9. **show pppoe redundancy**
10. **debug pppatm redundancy**
11. **debug pppoe redundancy**

DETAILED STEPS

Step 1 **show ccm clients**

Example:

```
This command is useful for troubleshooting the CCM synchronization component. This command
displays information about the CCM, which is the HA component that manages the capability to
synchronize session launch on the standby processor of a redundant processor HA system.
```

Active Route Processor

Example:

```
Router# show ccm clients
CCM bundles sent since peer up:
Sent Queued for flow control
Sync Session 16000 0
Update Session 0 0
Active Bulk Sync End 1 0
Session Down 0 0
ISSU client msgs 346 0
Dynamic Session Sync 0 0
Unknown msgs 0 0
Client events sent since peer up:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

Standby Route Processor

Example:

```
Router# show ccm clients

CCM bundles rcvd since last boot:
Sync Session 16000
Update Session 0
Active Bulk Sync End 1
Session Down 0
ISSU client msgs 173
Dynamic Session Sync 0
Unknown msgs 0
Client events extracted since last boot:
PPP 144000
PPPoE 96002
VPDN FSP 0
AAA 64000
PPP SIP 0
LTERM 16000
AC 0
L2TP CC 0
SSS FM 16000
VPDN LNS 0
```

Step 2 show ccm sessions

This command is useful for troubleshooting the CCM synchronization component. This command shows information about sessions managed by CCM.

Active Route Processor

Example:

```
Router# show ccm sessions
Global CCM state: CCM HA Active - Dynamic Sync
Global ISSU state: Compatible, Clients Cap 0x9EFFE
Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 9279
Number of sessions in state Ready: 0 0 6721
Number of sessions in state Dyn Sync: 16000 16000 0
Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 64 - -
Dynamic CPU 00:00:10 - 0 90 0
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 475 - -
```

Standby Route Processor

Example:

```
Router# show ccm sessions

Global CCM state: CCM HA Standby - Collecting
Global ISSU state: Compatible, Clients Cap 0x9EFFE
Current Bulk Sent Bulk Rcvd
----------- ----------- -----------
Number of sessions in state Down: 0 0 0
Number of sessions in state Not Ready: 0 0 8384
Number of sessions in state Ready: 16000 0 7616
Number of sessions in state Dyn Sync: 0 0 0
Timeout: Timer Type Delay Remaining Starts CPU Limit CPU Last
------------ -------- --------- ----------- --------- --------
Rate 00:00:01 - 0 - -
Dynamic CPU 00:00:10 - 0 90 0
```

```
Bulk Time Li 00:08:00 - 1 - -
RF Notif Ext 00:00:01 - 0 - -
```

Step 3 show ppp subscriber statistics

This command is useful for reviewing PPPoX session statistics. Use the **show ppp subscriber statistics** command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the **clear ppp subscriber statistics** command was last issued.

The following is sample output from the **show ppp subscriber statistics** command:

Example:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       7             7
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        0             0
PPPBindResp                    7             7
PPPReneg                       3             3
RestartTimeout                 5             5
PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  4             4
IDB CSTATE DOWN                8             8
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 8             8
```

Step 4 **show pppatm statistics**

This command is useful for obtaining statistics for PPPoA sessions. Use the **show pppatm statistics** command to display a total count of PPPoA events since the **clear pppatm statistics**command was last issued.

The following example displays PPPoA statistics:

Example:

```
Router# show pppatm statistics
    4000 : Context Allocated events
    3999 : SSS Request events
    7998 : SSS Msg events
    3999 : PPP Msg events
    3998 : Up Pending events
    3998 : Up Dequeued events
    3998 : Processing Up events
    3999 : Vaccess Up events
    3999 : AAA unique id allocated events
    3999 : No AAA method list set events
    3999 : AAA gets nas port details events
    3999 : AAA gets retrived attrs events
    68202 : AAA gets dynamic attrs events
    3999 : Access IE allocated events
```

Step 5 **show pppoe statistics**

This command is useful for reviewing PPPoX session statistics. Use the **show pppoe statistics** command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the **clear pppoe statistics** command was last issued.

The following is sample output from the **show pppoe statistics** command:

Example:

```
Router# show pppoe statistics
PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              0             0
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM DISCONNECT                 0             0
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        0             0
PPPoE Handles Freed            0             0
Dynamic Bind Request           0             0
Static Bind Request            0             0
```

Step 6 **show vpdn redundancy**

Use this command to verify the failure of any L2TP tunnels.

Example:

```
Router# show vpdn redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
Checkpoint Messaging on: FALSE
Standby RP is up: TRUE
Recv'd Message Count: 0
L2TP Tunnels: 2/2/2/0 (total/HA-enabled/HA-est/resync)
L2TP Sessions: 10/10/10 (total/HA-enabled/HA-est)
L2TP Resynced Tunnels: 0/0 (success/fail)
```

Step 7 **show vpdn history failure**

Use this command to verify the failure of any VPDN groups.

Example:

```
Router# show vpdn history failure

% VPDN user failure table is empty
```

Step 8 **show pppatm redundancy**

Use the **show pppatm redundancy** command to display the PPPoA HA sessions summary. The following is sample output from the **show pppatm redundancy** command from a Cisco 10000 series router standby processor:

Example:

```
Router-stby# show pppatm redundancy
0 : Session recreate requests from CCM
0 : Session up events invoked
0 : Sessions reaching PTA
0 : Sessions closed by CCM
0 : Session down events invoked
0 : Queued sessions waiting for base hwidb creation
0 : Sessions queued for VC up notification so far
0 : Sessions queued for VC encap change notification so far
0 : VC activation notifications received from ATM
0 : VC encap change notifications received from ATM
0 : Total queued sessions waiting for VC notification(Encap change+VC Activation)
```

Step 9 **show pppoe redundancy**

This command is useful for reviewing PPPoX session statistics. Use the **show pppoe redundancy** command to display statistics and events for PPPoE sessions. This command gives a cumulative count of PPPoE events and statistics, and an incremental count since the **clear pppoe redundancy** command was last issued.

The following is sample output from the **show pppoe redundancy** command from a Cisco 10000 series router standby processor:

Example:

```
Router-stby# show pppoe redundancy
12 Event Queues
size max kicks starts false suspends ticks(ms)
9 PPPoE CCM EV 0 1 2 3 1 0 20
Event Names
Events Queued MaxQueued Suspends usec/evt max/evt
1* 9 Recreate UP 2 0 1 0 1500 3000
2* 9 Recreate DOWN 0 0 0 0 0 0
3* 9 VC Wait UP 0 0 0 0 0 0
4* 9 VC Wait Encap 0 0 0 0 0 0
Sessions waiting for Base Vaccess: 0
Sessions waiting for ATM VC UP: 0
Sessions waiting for Auto VC Encap 0
```

Step 10 **debug pppatm redundancy**

Use the **debug pppatm redundancy** command to display CCM events and messages for PPPoA sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes. The following is sample output from the **debug pppatm redundancy** command from a Cisco 10000 series router active processor:

Example:

```
Router# debug pppatm redundancy
PPP over ATM redundancy debugging is on
```

Step 11 **debug pppoe redundancy**

Use the **debug pppoe redundancy** command to display CCM events and messages for PPPoE sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppoe redundancy
Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

Configuration Examples for Broadband High Availability Stateful Switchover

Example Configuring Broadband High Availability Stateful Switchover

The following example shows how to configure the Broadband High Availability Stateful Switchover feature:

```
Router# configure terminal
Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30
Router(config)# exit
```

The following is a sample configuration of PPPoX terminated into an RA-MPLS network with SSO. Commands that appear in the configuration task tables for this feature but that do not appear in the running configuration output are configured for their default settings.

```
Router# show running-config
hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
```

```
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

The following lines show the subscriber redundancy policy configuration:

```
subscriber redundancy dynamic limit cpu 90 delay 10
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
  virtual-template 2
!
bba-group pppoe grp3
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 10.1.1.1 255.255.255.255
!
interface Loopback100
  ip address 192.168.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
```

```
encapsulation dot1Q 2
pppoe enable group grp2
!
!
interface GigabitEthernet1/0/1
no ip address
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
encapsulation dot1Q 2
pppoe enable group grp5
!
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
!
interface GigabitEthernet7/0/3
no ip address
!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
```

```
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
  network 224.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 224.0.0.3 remote-as 1
  neighbor 224.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 224.0.0.3 activate
```

```
  neighbor 224.0.0.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.13.1.1 10.13.16.160
ip local pool pool4 10.14.1.1 10.14.16.160
ip local pool pool5 10.15.1.1 10.15.16.160
ip local pool pool6 10.16.1.1 10.16.16.160
ip local pool pool7 10.17.1.1 10.17.16.160
ip local pool pool8 10.18.1.1 10.18.16.160
ip classless !
!
no ip http server
!
!
arp 10.20.1.1 0020.0001.0001 ARPA
arp vrf vrf1 10.20.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS Broadband Access Aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
High Availability	"High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide
Performing an ISSU	The following chapters in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide : • "Cisco IOS XE Software Package Compatibility for ISSU" • "In Service Software Upgrade (ISSU)"
Broadband ISSU	"Broadband High Availability In Service Software Upgrade" module

Related Topic	Document Title
Stateful switchover	"Stateful Switchover" module
Configuring nonstop forwarding	"Configuring Nonstop Forwarding" module
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief" module

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Broadband High Availability Stateful Switchover

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

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

Table 26 Feature Information for the Broadband High Availability Stateful Switchover Feature

Feature Name	Releases	Feature Information
SSO--PPPoA	Cisco IOS XE Release 3.3S	In Cisco IOS XE Release 3.3S, this feature was implemented on ASR 1000 Series Routers. The Broadband High Availability Stateful Switchover feature delivers stateful switchover capability for PPP over ATM (PPPoA) sessions during RP switchover. The following commands were introduced or modified: **subscriber redundancy**, **debug pppatm redundancy**, **debug pppoe redundancy**, **show pppoe redundancy**, **show pppatm statistics**.

Feature Name	Releases	Feature Information
SSO--PPPoE	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5	In Cisco IOS XE Release 2.1, this feature was implemented on ASR 1000 Series Routers. This feature uses the SSO--PPPoE feature to provide the capability for dual Route Processor systems to support stateful switchover of PPPoX sessions and allow applications and features to maintain state while system control and routing protocol execution is transferred between an active and a standby processor. The following commands were introduced or modified: **clear ppp subscriber statistics**, **clear pppoe statistics**, **debug pppoe redundancy, show ccm clients, show ccm sessions, show ppp subscriber statistics, show pppoe statistic, subscriber redundancy**.

Broadband High Availability In-Service Software Upgrade

The Broadband High Availability (HA) In-Service Software Upgrade (ISSU) feature ensures continuous operations of broadband access protocols during software upgrades, downgrades, and service enhancements.

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 Table at the end of this document.

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

Prerequisites for 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 258
- Supported Broadband Aggregation Protocols, page 259
- Benefits of Broadband High Availability In-Service Software Upgrade, page 260

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, page 261.

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, page 259

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 259
- ISSU L2TP, page 259
- ISSU PPPoE, page 259
- ISSU RA-MLPS VPN, page 259

ISSU PPPoA

The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPP over ATM (PPPoA) sessions during supported software upgrades, downgrades, and enhancements.

ISSU L2TP

The L2TP HA Session SSO/ISSU on a LAC/LNS feature provides a generic SSO/ISSU mechanism for Layer 2 Tunneling Protocol (L2TP) on a Layer 2 Access Concentrator (LAC) and a Layer 2 Network Server (LNS). This feature preserves all fully established PPP and L2TP sessions during an SSO switchover or an ISSU upgrade or downgrade.

ISSU PPPoE

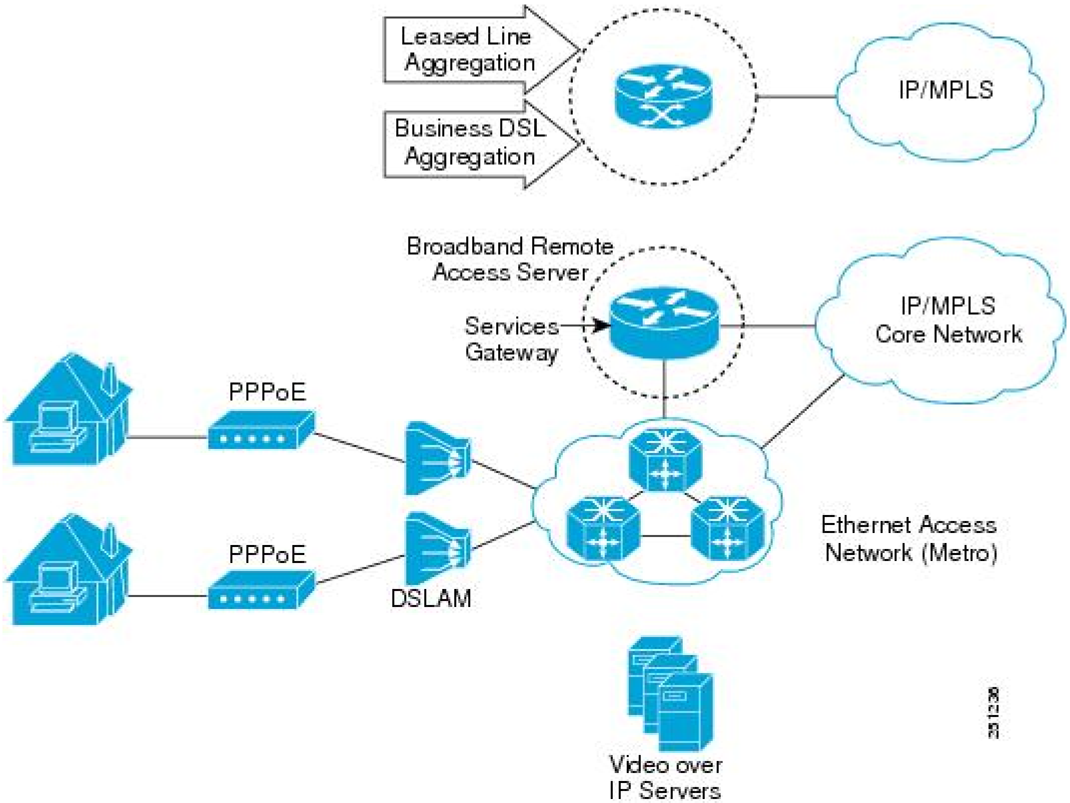
The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPP over Ethernet (PPPoE) subscriber access sessions, including PPPoE, PPPoE over VLAN, and PPPoE over QinQ sessions, during supported software upgrades, downgrades, and enhancements.

ISSU RA-MLPS VPN

The Broadband High Availability In-Service Software Upgrade feature delivers ISSU capability for PPPoA and PPPoE (PPPoX) sessions terminated into remote access (RA)-Multiprotocol Label Switching (MPLS) VPN or PPPoX into MPLS VPN during supported software upgrades, downgrades, and enhancements.

The figure below shows a typical broadband aggregation HA deployment with ISSU functionality.

Figure 14 ***Broadband Aggregation High Availability Deployment***



Benefits of Broadband High Availability In-Service Software Upgrade

- Eliminates network downtime for Cisco IOS XE software upgrades.
- Eliminates resource scheduling challenges associated with planned outages and late night maintenance windows.
- Accelerates deployment of new services and applications and allows faster implementation of new features, hardware, and fixes.
- Reduces operating costs due to outages while delivering higher service levels.
- Provides additional options for adjusting maintenance windows.
- Minimizes the impact of upgrades to service and allows for faster upgrades, resulting in higher availability.

How to Configure Broadband High Availability In-Service Software Upgrade

• Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA ISSU, page 262

Configuring Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade

The Broadband High Availability In-Service Software Upgrade feature is enabled by default. This task configures subscriber redundancy policy for HA ISSU capability, allowing you to manage synchronization between HA active and standby processors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber redundancy** {**bulk limit**{**cpu percentage delay** *delay-time* [**allow value**] | **time** *seconds* | **delay** *delay-time* | **dynamic limit cpu percentage delay** *delay-time* [**allow value] | rate sessions time}**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**subscriber redundancy** {**bulk limit**{**cpu percentage delay** *delay-time* [**allow value**] | **time** *seconds* | **delay** *delay-time* | **dynamic limit cpu percentage delay** *delay-time* [**allow value] | rate sessions time}** **Example:** `Router(config)# subscriber redundancy bulk limit cpu 75 delay 20 allow 30`	(Optional) Configures subscriber redundancy policy.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying and Troubleshooting Subscriber Redundancy Policy for Broadband HA ISSU

To verify the subscriber redundancy policy configuration, use the **show running-config** command. Sample output is available in the Configuration Examples for Broadband High Availability In-Service Software Upgrade, page 267.

- Step 1, Step 2 and Step 3 are useful for troubleshooting the CCM synchronization component.
- Step 4, Step 5 and Step 6 are useful for reviewing PPPoX session statistics.
- Step 7 and Step 8 are useful for verifying the failure of any L2TP tunnels or VPDN groups.
- Step 9 and Step 10 are typically used by Cisco engineers for internal debugging purposes.

SUMMARY STEPS

1. **show ccm clients**
2. **show ccm sessions**
3. **show ccm queues**
4. **show ppp subscriber statistics**
5. **show pppatm statistics**
6. **show pppoe statistics**
7. **show vpdn redundancy**
8. **show vpdn history failure**
9. **debug pppatm redundancy**
10. **debug pppoe redundancy**

DETAILED STEPS

Step 1 **show ccm clients**

This command displays information about the CCM, the HA component that manages the capability to synchronize session launch on the standby processor of a redundant processor HA system. Use the **show ccm clients** command to display information about CCM clients.

Example:

```
Router# show ccm clients
CCM bundles sent since peer up:
                                        Sent            Queued for flow control
    Sync Session                        0               0
    Update Session                      0               0
    Active Bulk Sync End                1               0
    Session Down                        0               0
    ISSU client msgs                    350             0
    Dynamic Session Sync                0               0
    Unknown msgs                        0               0
Client events sent since peer up:
    PPP                                 0
    PPPoE                               0
    VPDN FSP                            0
    AAA                                 0
    PPP SIP                             0
    LTERM                               0
    AC                                  0
```

```
    L2TP CC                         0
    SSS FM                          0
    IP SIP                          0
    IP IF                           0
    COA                             0
    Auto Svc                        0
    VPDN LNS                        0
```

Step 2 **show ccm sessions**

This command displays information about sessions managed by CCM.

Example:

```
Router# show ccm sessions

Global CCM state:                         CCM HA Active - Dynamic Sync
Global ISSU state:                        Compatible, Clients Cap 0x9EFFE
                                          Current     Bulk Sent   Bulk Rcvd
                                          ----------- ----------- -----------
Number of sessions in state Down:         0           0           0
Number of sessions in state Not Ready:    0           0           0
Number of sessions in state Ready:        0           0           0
Number of sessions in state Dyn Sync:     0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk CPU Lim 00:00:10 -         0           90        0
         Bulk Time Li 00:00:01 -         0           -         -
         RF Notif Ext 00:00:01 -         8           -         -
```

Step 3 **show ccm queues**

Use the **show ccm queues** command to display queue statistics for CCM sessions on active and standby processors. This command is primarily used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# show ccm queues
11 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 3 CCM              0     8         82         83        1          0         20
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  3 Sync Session           0        0         0         0         0         0
 2  3 Sync Client            0        0         0         0         0         0
 3  3 Update                 0        0         0         0         0         0
 4  3 Session Down           0        0         0         0         0         0
 5  3 Bulk Sync Begi         1        0         1         0         0         0
 6  3 Bulk Sync Cont         2        0         2         0         0         0
 7  3 Bulk Sync End          1        0         1         0         0         0
 8  3 Rcv Bulk End           0        0         0         0         0         0
 9  3 Dynamic Sync C         0        0         0         0         0         0
10  3 Going Active           0        0         0         0         0         0
11  3 Going Standby          0        0         0         0         0         0
12  3 Standby Presen         1        0         1         0         0         0
13  3 Standby Gone           0        0         0         0         0         0
15  3 CP Message           205        0         8         0       141      1000
16  3 Recr Session           0        0         0         0         0         0
17  3 Recr Update            0        0         0         0         0         0
18  3 Recr Sess Down         0        0         0         0         0         0
19  3 ISSU Session N         1        0         1         0         0         0
20  3 ISSU Peer Comm         0        0         0         0         0         0
21  3 Free Session           0        0         0         0         0         0
22  3 Sync Dyn Sessi         0        0         0         0         0         0
23  3 Recr Dyn Sessi         0        0         0         0         0         0
24  3 Session Ready          0        0         0         0         0         0
25  3 Pending Update         0        0         0         0         0         0
```

```
FSM Event Names          Events
 0    Invalid                 0
 1    All Ready               0
 2    Required Not Re         0
 3    Update                  0
 4    Down                    0
 5    Error                   0
 6    Ready                   0
 7    Not Syncable            0
 8    Recreate Down           0
```

Step 4 **show ppp subscriber statistics**

This command is useful for displaying events and statistics for PPP subscribers. Use the **show ppp subscriber statistics** command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the **clear ppp subscriber statistics** command was last issued.

Example:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        0             0
CstateUp                       7             7
CstateDown                     4             4
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       7             7
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        0             0
PPPBindResp                    7             7
PPPReneg                       3             3
RestartTimeout                 5             5
PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  4             4
IDB CSTATE DOWN                8             8
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 8             8
```

Step 5 **show pppatm statistics**

This command is useful for obtaining statistics for PPPoA sessions. Use the **show pppatm statistics** command to display a total count of PPPoA events since the **clear pppatm statistics**command was last issued.

Example:

```
Router# show pppatm statistics
    4000 : Context Allocated events
    3999 : SSS Request events
    7998 : SSS Msg events
    3999 : PPP Msg events
    3998 : Up Pending events
    3998 : Up Dequeued events
    3998 : Processing Up events
    3999 : Vaccess Up events
    3999 : AAA unique id allocated events
    3999 : No AAA method list set events
    3999 : AAA gets nas port details events
    3999 : AAA gets retrived attrs events
```

```
    68202 : AAA gets dynamic attrs events
    3999 : Access IE allocated events
```

Step 6 **show pppoe statistics**

This command is useful for obtaining statistics and events for PPPoE sessions. Use the **show pppoe statistics** command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the last time the **clear pppoe statistics** command was issued.

Example:

```
Router# show pppoe statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          5             5
DeEncap                        2             2
CstateUp                       0             0
CstateDown                     0             0
FastStart                      0             0
LocalTerm                      0             0
LocalTermVP                    0             0
MoreKeys                       0             0
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        0             0
PPPBindResp                    0             0
PPPReneg                       0             0
RestartTimeout                 2             2
PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  0             0
IDB CSTATE DOWN                0             0
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 0             0
ASR1006-1#sh pppoe statis
ASR1006-1#sh pppoe statistics ?
  |  Output modifiers
  <cr>
ASR1006-1#sh pppoe statistics
PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              0             0
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  0             0
SSS DISCONNECT                 0             0
SSS DISCONNECT ACK             0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           0             0
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                0             0
SSM UPDATED                    0             0
SSM ACCT STATS UPDATED         0             0
SSM DISCONNECT                 0             0
                               0             0
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    0             0
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        0             0
PPPoE Handles Freed            0             0
```

```
Dynamic Bind Request          0            0
Static Bind Request           0            0
SSM Async Stats Request       0            0
```

Step 7 **show vpdn redundancy**

Use this command to verify the failure of any L2TP tunnels.

Example:

```
Router# show vpdn redundancy

L2TP HA support: Silent Failover
L2TP HA Status:
  Checkpoint Messaging on: TRUE
  Standby RP is up:        TRUE
  Recv'd Message Count:    0
  L2TP Tunnels:            0/0/0/0 (total/HA-enabled/HA-est/resync)
  L2TP Sessions:           0/0/0 (total/HA-enabled/HA-est)
  L2TP Resynced Tunnels:   0/0 (success/fail)
```

Step 8 **show vpdn history failure**

Use this command to verify the failure of any VPDN groups.

Example:

```
Router# show vpdn history failure

% VPDN user failure table is empty
```

Step 9 **debug pppatm redundancy**

Use the **debug pppatm redundancy** command to display CCM events and messages for PPPoA sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppatm redundancy
*Dec  3 02:58:40.784: PPPATM HA: [14000001]: Received the first SHDB
*Dec  3 02:58:40.784: PPPATM HA: [14000001]: Base hwidb not created > yet, queuing SHDB *Dec  3
02:58:40.784: PPPATM HA: [14000001]:
Requesting base vaccess creation
```

Step 10 **debug pppoe redundancy**

Use the **debug pppoe redundancy** command to display CCM events and messages for PPPoE sessions on HA systems. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Example:

```
Router# debug pppoe redundancy
Nov 22 17:21:11.327: PPPoE HA[0xBE000008] 9: Session ready to sync data
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: Sync collection for ready events
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PADR, length = 58
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SESSION ID, length = 2
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SWITCH HDL, length = 4
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = SEGMENT HDL, length = 4
```

```
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = PHY SWIDB DESC, length = 20
Nov 22 17:21:11.351: PPPoE HA[0xBE000008] 9: code = VACCESS DESC, length = 28
```

Configuration Examples for Broadband High Availability In-Service Software Upgrade

Example Subscriber Redundancy Policy for Broadband High Availability In-Service Software Upgrade

The following example shows how to configure the Broadband High Availability In-Service Software Upgrade feature:

```
enable
configure terminal
subscriber redundancy bulk limit cpu 75 delay 20 allow 30
end
```

The following is a sample configuration of PPPoX terminated into an RA-MPLS network with SSO. Commands that appear in the configuration task tables for this feature but that do not appear in the running configuration output are configured for their default settings.

```
hostname Router
!
boot-start-marker
boot system bootflash:packages.conf !
enable password cisco
!
aaa new-model
!
!
aaa authentication ppp default local
!
!
!
aaa session-id common
ppp hold-queue 80000
ip subnet-zero
no ip gratuitous-arps
no ip domain lookup
ip vrf vrf1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
no ip dhcp use vrf connected
!
!
!
!
no subscriber policy recording rules
```

The following lines show subscriber redundancy policy configuration:

```
subscriber redundancy dynamic limit cpu 90 delay 10
subscriber redundancy bulk limit cpu 90 delay 10
subscriber redundancy rate 4000 1
subscriber redundancy delay 10
no mpls traffic-eng
mpls ldp graceful-restart
mpls ldp router-id Loopback100
no virtual-template snmp
no issu config-sync policy bulk prc
no issu config-sync policy bulk bem
!
redundancy mode sso
username cisco password 0 cisco
!
buffers small permanent 15000
buffers middle permanent 12000
buffers large permanent 1000
bba-group pppoe grp1
  virtual-template 1
!
bba-group pppoe grp2
  virtual-template 2
!
bba-group pppoe grp3
  virtual-template 3
!
bba-group pppoe grp4
  virtual-template 4
!
bba-group pppoe grp5
  virtual-template 5
!
bba-group pppoe grp7
  virtual-template 7
!
bba-group pppoe grp8
  virtual-template 8
!
bba-group pppoe grp6
  virtual-template 6
!
!
interface Loopback0
  ip vrf forwarding vrf1
  ip address 172.16.1.1 255.255.255.255
!
interface Loopback100
  ip address 172.31.0.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 192.168.2.26 255.255.255.0
  speed 100
  full-duplex
!
interface GigabitEthernet1/0/0
no ip address
load-interval 30
!
interface GigabitEthernet1/0/0.1
encapsulation dot1Q 2
pppoe enable group grp1
!
!
interface GigabitEthernet1/0/0.2
encapsulation dot1Q 2
pppoe enable group grp2
!
!
interface GigabitEthernet1/0/1
no ip address
```

```
!
interface GigabitEthernet1/0/1.1
encapsulation dot1Q 2
pppoe enable group grp3
!
!
interface GigabitEthernet1/0/1.2
encapsulation dot1Q 2
pppoe enable group grp4
!
!
interface GigabitEthernet1/0/2
no ip address
!
interface GigabitEthernet1/0/2.1
encapsulation dot1Q 2
pppoe enable group grp5
!
!
interface GigabitEthernet1/0/2.2
encapsulation dot1Q 2
pppoe enable group grp6
!
!
interface GigabitEthernet1/0/3
no ip address
!
interface GigabitEthernet1/0/3.1
encapsulation dot1Q 2
pppoe enable group grp7
!
!
interface GigabitEthernet1/0/3.2
encapsulation dot1Q 2
pppoe enable group grp8
!
interface GigabitEthernet7/0/3
no ip address
!
interface GigabitEthernet8/0/0
  mac-address 0011.0022.0033
  ip vrf forwarding vrf1
  ip address 10.1.1.2 255.255.255.0
  negotiation auto
!
interface GigabitEthernet8/1/0
  ip address 10.1.1.1 255.255.255.0
  negotiation auto
  mpls ip
!
interface Virtual-Template1
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool1
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template2
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool2
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template3
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool3
```

```
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template4
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool4
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template5
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool5
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template6
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool6
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template7
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool7
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
interface Virtual-Template8
  ip vrf forwarding vrf1
  ip unnumbered Loopback0
  no logging event link-status
  peer default ip address pool pool8
  no snmp trap link-status
  keepalive 30
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  nsf
  network 10.1.1.0 0.0.0.255 area 0
  network 10.0.0.0 0.0.0.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 10.0.0.3 remote-as 1
  neighbor 10.0.0.3 update-source Loopback100
  no auto-summary
  !
  address-family vpnv4
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
```

```
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool pool2 10.1.1.1 10.1.16.160
ip local pool pool3 10.1.1.1 10.1.16.160
ip local pool pool4 10.1.1.1 10.1.16.160
ip local pool pool5 10.1.1.1 10.1.16.160
ip local pool pool6 10.1.1.1 10.1.16.160
ip local pool pool7 10.1.1.1 10.1.16.160
ip local pool pool8 10.1.1.1 10.1.16.160
ip classless !
!
no ip http server
!
!
arp 10.1.1.1 0020.0001.0001 ARPA
arp vrf vrf1 10.1.1.1 0020.0001.0001 ARPA !
!
!
line con 0
line aux 0
line vty 0 4
  password cisco
!
exception crashinfo file bootflash:crash.log !
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Broadband commands	Cisco IOS Broadband Access Aggregation and DSL Command Reference
High Availability	"High Availability Overview" chapter in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide
Performing an ISSU	The following chapters in the Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide : • "Cisco IOS XE Software Package Compatibility for ISSU" • "In Service Software Upgrade (ISSU)"
Broadband SSO	Broadband High Availability Stateful Switchover
Stateful switchover	Stateful Switchover
Cisco nonstop forwarding	Cisco Nonstop Forwarding
Layer 2 Tunnel Protocol	Layer 2 Tunnel Protocol Technology Brief

Related Topic	Document Title
Additional information about commands used in this document	• *Cisco IOS Broadband Access Aggregation and DSL Command Reference* • Cisco IOS Master Command List, All Releases

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for Broadband High Availability In-Service Software Upgrade

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

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

Table 27 Feature Information for Cisco IOS Broadband High Availability In-Service Software Upgrade

Feature Name	Releases	Feature Information
ISSU-PPPoA	Cisco IOS XE Release 3.3S	This feature was introduced on Cisco ASR 1000 Series Routers. This feature uses the ISSU support for PPPoA to ensure continuous operations of broadband access protocols during software upgrades. The following commands were introduced or modified: **debug pppatm redundancy** , **debug pppoe redundancy**, **show pppoe redundancy**, **show pppatm redundancy**, **show pppatm statistics**, **subscriber redundancy**

Feature Name	Releases	Feature Information
ISSU--PPPoE	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5	This feature was introduced on Cisco ASR 1000 Series Routers. This feature uses the ISSU--PPPoE support to ensure continuous operations of broadband access protocols during software upgrades, downgrades, and service enhancements. The following commands were introduced or modified: **clear ppp subscriber statistics**, **clear pppoe statistics**, **debug pppoe redundancy, show ccm clients, show ccm sessions, show ppp subscriber statistics, show pppoe statistic, subscriber redundancy**

Controlling Subscriber Bandwidth

The Dynamic Subscriber Bandwidth Selection (DBS) feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM quality of service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) session is established.

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 Table at the end of this document.

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

Prerequisites for Controlling Subscriber Bandwidth

A Cisco ASR 1000 series router must have the following shared port adapters (SPAs) installed to enable DBS:

- SPA-3XOC3-ATM-V2
- SPA-1XOC3-ATM-V2
- SPA-1XOC12-ATM-V2

Restrictions for Controlling Subscriber Bandwidth

The DBS feature does not support the following:

- Switched virtual circuits (SVC)
- ATM port adapters installed in a Cisco ASR 1000 series router
- When changing QoS values dynamically on a VC, there can be some duration (in milliseconds) during which traffic on the VC is dropped.

Information About Controlling Subscriber Bandwidth

Traffic-Shaping Parameters

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic-shaping parameters to be dynamically changed based on the RADIUS profile of a PPPoE or PPPoA user logging in on the PVC. If the user is the first user on a given PVC, the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all the sessions are selected as the PCR and SCR, respectively, of the VC.

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Traffic-shaping parameters can be locally configured by Cisco IOS command-line interface (CLI) in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic-shaping parameters that are CLI-configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overridden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a "QoS-management" string via vendor-specific attribute (VSA) 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for a particular user or domain. If the QoS specified for a domain or user cannot be applied on the PVC to which the session belongs, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** command to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you configure the **no dbs enable** command on a VC, additional sessions that are configured will display DBS-configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessions are already up on the VC, all sessions on that VC have DBS QoS parameters.

Benefits of Controlling Subscriber Bandwidth

DBS provides the following benefits:

- Wholesale service providers can provide different bandwidth options to their retail service provider customers, such as ISPs and enterprises.
- Subscribers can choose between enhanced and basic service, with a fixed billing plan for each service.

How to Control Subscriber Bandwidth

Configuring DBS Under a VC Class

Perform the following task to configure DBS under a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **dbs enable**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm class1`	Creates an ATM VC class and enters ATM VC class configuration mode. • A VC class can be applied to an ATM interface, subinterface, or VC.
Step 4	**dbs enable** **Example:** `Router(config-vc-class)# dbs enable`	Applies DBS QoS parameters.

Configuring DBS on a PVC

Perform the following task to configure DBS for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **pvc** [*name*] *vpi* /*vci*
5. **dbs enable**
6. **protocol pppoe**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**pvc** [*name*] *vpi* /*vci* **Example:** `Router(config-if)# pvc` **2/101**	Specifies an ATM PVC and creates or assigns a name to an ATM PVC, and enters interface-ATM-VC configuration mode. **Note** The arguments *vpi* and *vci* cannot both be set to 0; if one is 0, the other cannot be 0.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Applies DBS QoS parameters.
Step 6	**protocol pppoe** **Example:** `Router(config-if-atm-vc)# protocol pppoe`	Specifies PPPoE as the protocol of the ATM PVC.

Configuring DBS on a Range of PVCs

Perform this task to configure DBS for a range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **range**[*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /*end-vci*
5. **dbs enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**range**[*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /*end-vci* **Example:** `Router(config-subif)# range pvc 0/101 0/500 class-range pppoe`	Defines a range of ATM PVCs and enables PVC range configuration mode.
Step 5	**dbs enable** **Example:** `Router(config-if-atm-vc)# dbs enable`	Applies DBS QoS parameters.

Configuring DBS on a PVC Within a PVC Range

Perform this task to configure DBS for a specific PVC within a range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **in-range** [*pvc-name*] [[*vpi* /]*vci*]
6. **dbs enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 0/101 0/500 class-range pppoe`	Defines a range of ATM PVCs and enables PVC range configuration mode.
Step 5	**in-range** [*pvc-name*] [[*vpi* /]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range pvc1 3/104`	Defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.
Step 6	**dbs enable** **Example:** `Router(config-if-atm-range-pvc)# dbs enable`	Applies DBS QoS parameters.

Configuring the RADIUS Attributes for DBS

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Configure the RADIUS attributes listed in this section in the user or domain profiles on the authentication, authorization, and accounting (AAA) server. The user or domain profile is downloaded from the AAA server as part of user authentication.

The QoS management string for DBS has the following syntax:

```
Cisco-Avpair = atm:peak-cell-rate=155000
Cisco-Avpair = atm:sustainable-cell-rate=155000
```

You must configure the PCR. Configuring the SCR is optional. If you configure only the PCR, the ATM service type is an unspecified bit rate (UBR). If you specify both the SCR and the PCR, the ATM service type is a variable bit rate nonreal-time (VBR-nrt) connection.

If the peak rate is greater than the maximum rate permitted on the ATM physical interface, the PCR applied on the ATM PVC is set to the maximum rate. If the specified PCR is less than the minimum rate, then the PCR applied on the ATM PVC is the minimum rate.

If the sustainable-cell-rate (in Kbps) applied exceeds the maximum for the interface, the session is rejected.

Note DBS cannot change service categories such as from UBR to VBR-nrt. For details, see the table in Configuring Dynamic Suscriber Services .

Verifying DBS

Note The configuration examples in this section explain the PPPOE termination using a VPDN group.

SUMMARY STEPS

1. Enter the **show atm pvc** *vpi* / *vci*command to view details about ATM PVCs or VCs:
2. Enter the **show atm pvc dbs**command to display information about ATM PVCs that have DBS QoS parameters applied:
3. Enter the **show running-config** command to verify that DBS QoS parameters have been applied. If you enter the **dbs enable** or the **no dbs enable**command, it appears in the output of the **show running-config command**. If you enter the **default dbs enable**command, it does not appear.

DETAILED STEPS

Step 1 Enter the **show atm pvc** *vpi* / *vci*command to view details about ATM PVCs or VCs:

Example:

```
Router# show atm pvc 0/75
ATM1/0.4:VCD:1, VPI:0, VCI:75
UBR, PeakRate:149760
AAL5-LLC/SNAP, etype:0x0, Flags:0xC20, VCmode:0x0
OAM frequency:0 second(s), OAM retry frequency:1 second(s)
OAM up retry count:3, OAM down retry count:5
OAM Loopback status:OAM Disabled
OAM VC state:Not Managed
ILMI VC state:Not Managed
```

```
PA TxRingLimit:40 particles
PA Rx Limit:1600 particles
InARP frequency:15 minutes(s)
Transmit priority 4
InPkts:18, OutPkts:21, InBytes:1263, OutBytes:1476
InPRoc:18, OutPRoc:3
InFast:0, OutFast:0, InAS:0, OutAS:0
InPktDrops:0, OutPktDrops:0/0/0 (holdq/outputq/total)
CrcErrors:0, SarTimeOuts:0, OverSizedSDUs:0, LengthViolation:0,
CPIErrors:0
Out CLP=1 Pkts:0
OAM cells received:0
F5 InEndloop:0, F5 InSegloop:0, F5 InAIS:0, F5 InRDI:0
F4 InEndloop:0, F4 InSegloop:0, F4 InAIS:0, F4 InRDI:0
OAM cells sent:0
F5 OutEndloop:0, F5 OutSegloop:0, F5 OutRDI:0
F4 OutEndloop:0, F4 OutSegloop:0, F4 OutRDI:0
OAM cell drops:0
Status:UP
PPPOE enabled.
DBS enabled.
```

Step 2 Enter the **show atm pvc dbs**command to display information about ATM PVCs that have DBS QoS parameters applied:

Example:

```
Router# show atm pvc dbs
            VCD /                                     Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells
Sts
1/0.7      3            0    75   PVC    MUX      VBR    2000    700   94
UP
```

Step 3 Enter the **show running-config** command to verify that DBS QoS parameters have been applied. If you enter the **dbs enable** or the **no dbs enable**command, it appears in the output of the **show running-config command**. If you enter the **default dbs enable**command, it does not appear.

Example:

```
Router# show running-config
Building configuration...
Current configuration : 2902 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa session-id common
!
username usera password 0 password0
username lac password 0 password1
username lns password 0 password2
username nrp1 password 0 password3
username user1 password 0 password4
username nrp1-3 password 0 password5
username xyz@abc.com password 0 password6
ip subnet-zero
```

```
!
!
ip host dirt 172.69.1.129
ip host boot 172.19.192.254
!
vpdn enable
!
vpdn-group lac
 request-dialin
  protocol l2f
  domain pepsi.com
 initiate-to ip 10.1.1.5
 local name lac
!
vpdn-group pppoe_terminate
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 2000
 pppoe limit per-vc 2000
!
!
!
!
!
!
!
!
!
vc-class atm pppoa
  encapsulation aal5mux ppp Virtual-Template2
  dbs enable
!
vc-class atm pppoe
  dbs enable
  protocol pppoe
!
interface Loopback1
 no ip address
!
interface FastEthernet0/0
 ip address 10.0.74.211 255.255.255.0
 duplex half
 no cdp enable
!
interface ATM1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no atm ilmi-keepalive
 atm voice aal2 aggregate-svc upspeed-number 0
!
interface ATM1/0.4 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 pvc 0/75
  dbs enable
  protocol pppoe
 !
!
interface ATM1/0.5 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 pvc 0/85
 !
!
interface ATM1/0.7 point-to-point
 ip address 10.1.1.6 255.255.255.0
 no ip route-cache
 no ip mroute-cache
```

```
 pvc 0/95
  class-vc pppoa
  ubr 5000
 !
!
interface ATM1/0.10 point-to-point
 no ip route-cache
 no ip mroute-cache
 range pvc 0/101 0/500
  class-range pppoe
 !
  pvc-in-range 0/102
   no dbs enable
  !
!
interface Virtual-Template1
 ip unnumbered Loopback1
 ip mtu 1492
 no keepalive
 peer default ip address pool local_pool
 ppp authentication chap
!
interface Virtual-Template2
 ip address negotiated
 ip mtu 1492
 peer default ip address pool local_pool
 ppp authentication chap
!
interface Virtual-Template10
 ip address 192.168.11.1 255.255.255.0
 no keepalive
 peer default ip address pool p3
 ppp authentication chap
!
interface Virtual-Template11
 ip address negotiated
 no keepalive
 ppp chap hostname host1
 ppp chap password password1
!
ip local pool p3 192.168.0.0 192.170.12.250
ip local pool local_pool 150.10.3.1 150.10.10.250
ip default-gateway 10.0.74.1
ip classless
ip route 10.0.0.0 10.0.0.0 10.0.74.1
ip route 10.107.164.0 255.255.255.0 FastEthernet0/0
no ip http server
!
!
!
radius-server host 172.18.0.0 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 5 15
!
!
end
```

Monitoring DBS

Use the commands listed below to monitor DBS:

Command	Purpose
debug atm events	Displays the normal set of ATM events when a session comes up or goes down.
debug atm errors	Displays protocol errors and error statistics associated with VCs.
debug atm status	Displays changes in the status of a VC when a session comes up or goes down or when the VC configuration is changed.
debug ppp authentication	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
debug ppp error	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
debug ppp negotiation	Enables debugging of PPP negotiation process.
debug radius	Displays detailed debugging information associated with RADIUS.
debug vpdn event	Displays Layer 2 tunneling protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
debug vpdn l2x-errors	Displays Layer 2 forwarding protocol (L2F) and L2TP errors that prevent tunnel establishment or normal operation.
debug vpdn 12x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
show atm pvc	Displays all ATM PVCs and traffic information.
show atm pvc dbs	Displays ATM PVCs that have DBS QoS parameters applied.

Command	Purpose
show atm vc detailed	Displays information about ATM PVCs and SVCs.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.

Configuration Examples for Controlling Subscriber Bandwidth

Configuring DBS for a VC Class Example

In the following example, DBS QoS parameters have been applied to a VC called "cisco":

```
vc-class atm cisco
 dbs enable
```

Configuring DBS for a PVC Example

In the following example, DBS QoS parameters have been applied on a PVC called "cisco":

```
interface atm0/0/0.5 point-to-point
 ip address 10.0.0.0 255.255.255.0
 pvc cisco 0/100
 dbs enable
 protocol pppoe
```

Configuring DBS for a Range of PVCs Example

In the following example, DBS QoS parameters have been applied on a range of PVCs. The range is named "cisco range" and has a *start-vpi* of 0, a *start-vci* of 50, an *end-vpi*of 0, and an *end-vci* of 70:

```
interface atm0/0/0.1 multipoint
 ip address 10.0.0.0 255.255.255.0
 range cisco pvc 0/50 0/70
 dbs enable
```

Configuring DBS for a PVC Within a PVC Range Example

In the following example, DBS parameters have been applied on PVC 60, which is part of the PVC range called "cisco":

```
interface atm0/0/0.1 multipoint
```

```
range cisco pvc 0/50 0/70
pvc-in-range 0/60
dbs enable
```

Configuring RADIUS Attributes Examples

The following example shows how to configure RADIUS attributes for a domain profile for DBS:

```
cisco.com  Password = "cisco", Service-Type = Outbound
     Service-Type = Outbound,
     Cisco-Avpair = "vpdn:tunnel-id=tunnel33",
     Cisco-Avpair = "vpdn:tunnel-type=l2tp",
     Cisco-Avpair = "vpdn:l2tp-tunnel-password=password2",
     Cisco-Avpair = "vpdn:ip-addresses=172.16.0.0",
     Cisco-Avpair = "atm:peak-cell-rate=155000",
     Cisco-Avpair = "atm:sustainable-cell-rate=155000"
```

The following example shows how to configure RADIUS attributes for a user profile for DBS:

```
user1@cisco.com Password = "userpassword1", Service-Type = Outbound
     Service-Type = Outbound,
     Cisco-Avpair = "atm:peak-cell-rate=155000",
     Cisco-Avpair = "atm:sustainable-cell-rate=155000"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco Subscriber Edge Services Manager	Cisco Subscriber Edge Services Manager
Access Point Name Manager	APN Manager Application Programming Guide
RADIUS configuration	*"Configuring RADIUS" chapter of the Cisco IOS Security Configuration Guide*
RADIUS attributes	"RADIUS Attributes" appendix to the *Cisco IOS Security Configuration Guide*
Broadband access aggregation concepts	" Understanding Broadband Access Aggregation" *module*
Tasks for preparing for broadband access aggregation	" Preparing for Broadband Access Aggregation" *module*
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	"Wide-Area Networking Commands" in the *Cisco IOS Wide-Area Networking Command Reference*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

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

Feature Information for Controlling Subscriber Bandwidth

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

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

Table 28 Feature Information for Controlling Subscriber Bandwidth

Feature Name	Releases	Feature Configuration Information
Dynamic Subscriber Bandwidth Selection (DBS)	Cisco IOS XE Release 2.5	This feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM quality of service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.

PPPoE Service Selection

The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. You choose one of the services offered, and the service is provided when the PPPoE session becomes active. This feature enables service providers to offer a variety of services and to charge you according to the service chosen.

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 Table at the end of this document.

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

Prerequisites for PPPoE Service Selection

- PPPoE must be configured using PPPoE profile configuration rather than virtual private dial-up network (VPDN) group configuration as described in the "Providing Protocol Support for Broadband Aggregation of PPPoE Sessions" module.
- The PPPoE client must support service tags in the PPPoE discovery phase.
- The procedures in this document assume that RADIUS accounting and authentication, and PPPoE are configured and working, if you use PPPoE service selection to offer tunneling services.

Information About PPPoE Service Selection

PPPoE Service Selection Through Service Tags

PPPoE service selection enables a PPPoE server to offer clients a selection of services during call setup. The PPPoE client chooses one of the services offered, and that service is provided when the PPPoE session becomes active.

PPPoE service selection works through the exchange of service tags during the PPPoE discovery phase. When a client initiates a call with a PPPoE Active Discovery Initiation (PADI) packet, the PPPoE server responds with a PPPoE Active Discovery Offer (PADO) packet that advertises a list of available services. The client selects a service and sends a PPPoE Active Discovery Request (PADR) packet that indicates the service name that was selected.

When the PPPoE server receives the PADR packet that indicates the chosen service, the PPPoE server handles the service name in the same manner as a domain name. The service profile for the service name is retrieved from a RADIUS server, and the attributes within that service profile are applied to the call.

PPPoE Service Names

Each PPPoE service has a service name, which can be defined as a set of characteristics that are applied to a PPPoE connection when that service name is selected during call setup.

When you configure PPPoE service selection, you can define a RADIUS service profile for each service name, list in a subscriber profile the service names that you want to advertise, and then assign the subscriber profile to a PPPoE profile. The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

If a subscriber profile is not assigned to a PPPoE profile, the PPPoE connections that use that PPPoE profile are established without the additional service tags in the discovery packets. If a port is configured with a static service name (using the **vpn service** command), the static service name takes precedence, and no services are advertised to the client.

The Cisco RADIUS vendor-specific attribute (VSA) "service-name" is used in RADIUS accounting records to log the service name that was selected by the client. This attribute is also used to download the service names from the subscriber profile when the subscriber profile is defined on the RADIUS server.

RADIUS Service Profiles for PPPoE Service Selection

A service profile must be created on the RADIUS server for each service name. The service profile contains attributes that define how the call is handled. Currently, two sets of attributes are available for defining service profiles: attributes that define tunneling and attributes that define the quality of service (QoS) that is applied to the permanent virtual circuit (PVC) on which the PPPoE call is coming in.

The table below lists some of the attributes that are supported in RADIUS service profiles for PPPoE service selection.

Benefits of PPPoE Service Selection

PPPoE service selection enables a service provider to use PPPoE to offer a selection of services to you and to charge you according to the service selected. For example, a wholesaler could offer different levels of service by defining multiple service profiles for the same tunnel but with different levels of QoS for the ATM PVC. The wholesaler would be able to charge you according to the level of service provided.

PPPoE service selection could also be used by access providers to avoid link control protocol (LCP) negotiation at the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) for sessions that are to be forwarded to tunnels. Avoiding LCP negotiation at the LAC can improve scalability of the LAC during call setup and help alleviate the load on the LAC while all the sessions on the LAC are reconnecting after an outage.

Attributes Used to Define a RADIUS Service Profile for PPPoE Selection

The table below lists some of the attributes that can be used to define a RADIUS service profile for PPPoE service selection. These attributes are defined when setting up the RADIUS server.

Table 29 Attributes for the RADIUS Service Profile for PPPoE Service Selection

RADIUS Entry	Purpose
`User-Service-Type = Outbound-User`	Configures the service type as outbound.
`Cisco-AVpair = "vpdn:tunnel-id=` *`name`* **`"`**	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.
`Cisco-AVpair = "vpdn:tunnel-type=l2tp"`	Specifies Layer 2 Tunnel Protocol (L2TP).
`Cisco-AVpair = "vpdn:ip-addresses=` *`ip-address`* **`"`**	Specifies the IP address of L2TP network server (LNS).
`Cisco-AVpair = "atm:peak-cell-rate=` *`kbps`* **`"`**	Specifies the peak cell rate, in kbps, that is applied to the ATM PVC on which a PPPoE session is being established.
`Cisco-AVpair = "atm:sustainable-cell-rate=` *`kbps`* **`"`**	Specifies the sustainable cell rate, in kbps, that is applied to the ATM PVC on which a PPPoE session is being established.

Attributes Used to Configure a Subscriber Profile on the RADIUS Server for PPPoE Service Selection

The table below lists the attributes that can be used to configure a RADIUS subscriber profile to support PPPoE service selection.

The default AAA authorization method list determines where the policy manager looks for the subscriber profile. When the subscriber profile is configured remotely, the **aaa authorization network default group**

radiuscommand must be included in the AAA configuration so the policy manager knows to look for the subscriber policy on a AAA server. These attributes are defined while configuring the RADIUS server. Refer to the RADIUS server documentation for information about how to perform this configuration.

Table 30 Attributes for the RADIUS Subscriber Profile for PPPoE Service Selection

RADIUS Entry	Purpose
`User-Service-Type = Outbound-User`	Configures the service type as outbound.
`Cisco-AVpair = "pppoe:service-name=` *service-name* `"`	Specifies a PPPoE service name that is listed in this subscriber profile.

How to Offer PPPoE Service Selection

Configuring the Subscriber Profile for PPPoE Service Selection

The subscriber profile contains the list of services that is advertised to PPPoE clients. You can configure the subscriber profile locally on the router or on the RADIUS server. Perform this task to configure a local subscriber profile for PPPoE service selection.

The default AAA authorization method list determines where the policy manager looks for the subscriber profile. When the subscriber profile is configured locally, the **aaa authorization network default local** command must be included in the AAA configuration so the policy manager knows to look for the subscriber policy locally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **pppoe service** *service-name*
5. Repeat Step 4 for each service name that you want to add to the subscriber profile.
6. **end**
7. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service abc`	Enters service policy map configuration mode and creates or modifies a service policy map, which is used to define an Intelligent Services Gateway (ISG) subscriber service.
Step 4	**pppoe service** *service-name* **Example:** `Router(config-service-policymap)# pppoe service gold-isp-A`	Adds a PPPoE service name to a subscriber profile.
Step 5	Repeat Step 4 for each service name that you want to add to the subscriber profile.	--
Step 6	**end** **Example:** `Router(config-service-policymap)# end`	(Optional) Terminates the configuration session and returns to global configuration mode.
Step 7	end **Example:** `Router(config)#` **end**	(Optional) Exits global configuration mode.

Configuring the PPPoE Profile for PPPoE Service Selection

Perform this task to associate a subscriber profile with a PPPoE profile.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*group-name* | **global**}
4. **virtual-template** *template-number*
5. **sessions per-vc limit** *number*
6. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
7. **end**
8. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group1`	Defines a PPPoE profile and enters BBA group configuration mode. • The **global** keyword creates a profile that serves as the default profile for any PPPoE port that is not assigned a specific profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Specifies which virtual template is used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.
Step 5	**sessions per-vc limit** *number*	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile.

	Command or Action	Purpose
Step 6	**service profile** *subscriber-profile-name* [**refresh** *minutes*] **Example:** `Router(config-bba-group)# service profile subscriber-group1`	Assigns a subscriber profile to a PPPoE profile. • The PPPoE server advertises the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. • The PPPoE configuration that is derived from the subscriber gold_isp_A (where gold services created using the Cisco Distributed Administrative Tool (CDAT) interface are defined) under the PPPoE profile. Use the **service profile** command with the **refresh** keyword and the *minutes* argument to cause the cached PPPoE configuration to be timed out after a specified number of minutes.
Step 7	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Returns to global configuration mode.
Step 8	end **Example:** `Router(config)#` **end**	(Optional) Exits global configuration mode.

- Troubleshooting Tips, page 28
- What to Do Next, page 297

Troubleshooting Tips

Use the **show pppoe session** and **debug pppoe** commands to troubleshoot PPPoE sessions.

What to Do Next

Once a PPPoE profile has been defined, it must be assigned to a PPPoE port (Fast Ethernet, virtual LAN [VLAN], or PVC), a virtual circuit (VC) class, or an ATM PVC range. For more information about how to configure PPPoE profiles, refer to the Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions chapter.

Verifying PPPoE Service Selection

Perform this task to verify PPPoE service selection configuration and performance. Steps 2 through 3 are optional and do not have to be performed in a particular order.

SUMMARY STEPS

1. **show pppoe derived group** *group-name*
2. **show vpdn** [**session** [**all** | **packets** | **sequence** | **state**] | **tunnel** [**all** | **packets** | **summary** | **state** | **transport**]]
3. **show atm pvc** [*vpi* **/** *vci* | *name* | **interface atm** *slot*/*subslot*/*port*[**.** *subinterface* **multipoint**]] [**ppp**]

DETAILED STEPS

Step 1 **show pppoe derived group** *group-name*

(Optional) Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.

This command is useful for viewing the subscriber profile configuration when the subscriber profile is configured on a remote AAA server.

Example:

```
Router# show pppoe derived group sp-group-a
Derived configuration from subscriber profile 'abc':
Service names:
   isp-xyz, gold-isp-A, silver-isp-A
```

Step 2 **show vpdn** [**session** [**all** | **packets** | **sequence** | **state**] | **tunnel** [**all** | **packets** | **summary** | **state** | **transport**]]

(Optional) Displays information about active L2TP or Layer 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN.

Use this command to display tunneling parameters for the services configured for tunneling.

Example:

```
Router# show vpdn
Active L2F tunnels
NAS Name   Gateway Name    NAS CLID   Gateway CLID   State
nas        gateway           4             2          open
L2F MIDs
Name                NAS Name    Interface    MID      State
router1@cisco.com       nas          As7          1       open
router2@cisco.com        nas          As8          2       open
```

Step 3 **show atm pvc** [*vpi* **/** *vci* | *name* | **interface atm** *slot*/*subslot*/*port*[**.** *subinterface* **multipoint**]] [**ppp**]

(Optional) Displays all ATM PVCs and traffic information.

Use this command to display ATM QoS parameters for the services configured for ATM QoS.

Example:

```
Router# show atm pvc
           VCD/                                 Peak      Avg/Min   Burst
Interface  Name    VPI   VCI   Type   Encaps     Kbps        Kbps   Cells      Sts
2/0        1        0     5    PVC     SAAL     155000      155000             UP
2/0        2        0    16    PVC     ILMI     155000      155000             UP
2/0.2      101      0    50    PVC     SNAP     155000      155000             UP
2/0.2      102      0    60    PVC     SNAP     155000      155000           DOWN
2/0.2      104      0    80    PVC     SNAP     155000      155000             UP
2/0        hello    0    99    PVC     SNAP       1000
```

Monitoring and Maintaining PPPoE Service Selection

To monitor and maintain PPPoE service selection, perform the following steps.

SUMMARY STEPS

1. **clear pppoe derived group** *group-name*
2. **debug pppoe events** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]
3. **debug radius** [**brief** | **hex**]

DETAILED STEPS

Step 1 **clear pppoe derived group** *group-name*

Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.

Example:

```
Router# clear pppoe derived group group1
```

Step 2 **debug pppoe events** [**rmac** *remote-mac-address* | **interface** *type number* [**vc** {[*vpi* /]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

(Optional) Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.

Use this command to monitor the exchange of PPPoE service names during call setup.

Example:

```
Router# debug pppoe events interface atm 0/0.0 vc 101

PPPoE protocol events debugging is on
Router#
00:41:55:PPPoE 0:I PADI  R:00b0.c2e9.c470 L:ffff.ffff.ffff 0/101 ATM0/1/0.10
00:41:55:PPPoE 0:O PADO, R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:PPPoE 0:I PADR  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:PPPoE :encap string prepared
00:41:55:[3]PPPoE 3:Access IE handle allocated
00:41:55:[3]PPPoE 3:pppoe SSS switch updated
00:41:55:[3]PPPoE 3:AAA unique ID allocated
00:41:55:[3]PPPoE 3:No AAA accounting method list
00:41:55:[3]PPPoE 3:Service request sent to SSS
00:41:55:[3]PPPoE 3:Created  R:0001.c9f0.0c1c L:00b0.c2e9.c470 0/101 ATM0/1/0.10
00:41:55:[3]PPPoE 3:State REQ_NASPORT    Event MORE_KEYS
00:41:55:[3]PPPoE 3:O PADS  R:00b0.c2e9.c470 L:0001.c9f0.0c1c 0/101 ATM0/1/0.10
00:41:55:[3]PPPoE 3:State START_PPP    Event DYN_BIND
00:41:55:[3]PPPoE 3:data path set to PPP
00:41:57:[3]PPPoE 3:State LCP_NEGO    Event PPP_LOCAL
00:41:57:PPPoE 3/SB:Sent vtemplate request on base Vi2
00:41:57:[3]PPPoE 3:State CREATE_VA    Event VA_RESP
00:41:57:[3]PPPoE 3:Vi2.1 interface obtained
00:41:57:[3]PPPoE 3:State PTA_BIND    Event STAT_BIND
```

```
00:41:57:[3]PPPoE 3:data path set to Virtual Acess
00:41:57:[3]PPPoE 3:Connected PTA
```

Step 3 **debug radius** [**brief** | **hex**]

(Optional) Displays information associated with RADIUS.

Use this command to monitor the transactions between the router and the RADIUS server.

Example:

```
Router# debug radius

Radius protocol debugging is on
Radius packet hex dump debugging is off
Router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.0:0000, Accounting-Request, len
358
00:02:50: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:02:50: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS:  NAS-Port-Type       [61]  6   Async
00:02:50: RADIUS:  User-Name           [1]   12  "5559999999"
00:02:50: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:02:50: RADIUS:  Calling-Station-Id  [31]  12  "5559999999"
00:02:50: RADIUS:  Acct-Status-Type    [40]  6   Start
00:02:50: RADIUS:  Service-Type        [6]   6   Login
00:02:50: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:02:50: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS:  Vendor, Cisco       [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:02:50: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS:  Acct-Session-Id     [44]  10  "55559999"
00:02:50: RADIUS:  Delay-Time          [41]  6   0
00:02:51: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 5559000000
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 0.0.000.0:0000, Access-Request, len
171
00:03:01: RADIUS:  NAS-IP-Address      [4]   6   10.x.y.z
00:03:01: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:01: RADIUS:  User-Name           [1]   8   "123456"
00:03:01: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:01: RADIUS:  Calling-Station-Id  [31]  12  "555999999"
00:03:01: RADIUS:  User-Password       [2]   18  *
00:03:01: RADIUS:  Vendor, Cisco       [26]  36  VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 0 0.0.000.0 1:1823, Access-Accept, len 115
00:03:01: RADIUS:  Service-Type        [6]   6   Login
00:03:01: RADIUS:  Vendor, Cisco       [26]  29  VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS:  Vendor, Cisco       [26]  27  VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS:  Vendor, Cisco       [26]  26  VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS:  Class               [25]  7   6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 5559000000, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 0 0.0.000.0:0000, Accounting-Request,
len 775
00:03:13: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:13: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS:  NAS-Port-Type       [61]  6   Async
```

```
00:03:13: RADIUS:  User-Name           [1]   8   "123456"
00:03:13: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:03:13: RADIUS:  Calling-Station-Id  [31]  12  "5559000000"
00:03:13: RADIUS:  Acct-Status-Type    [40]  6   Stop
00:03:13: RADIUS:  Class               [25]  7   6C6F63616C
00:03:13: RADIUS:  Undebuggable        [45]  6   00000001
00:03:13: RADIUS:  Service-Type        [6]   6   Login
00:03:13: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS:  Vendor, Cisco       [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  59  VT=28 TL=53
h323-connect-time=*16:02:48.946 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  62  VT=29 TL=56in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  23  VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  21  VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-paks-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS:  Delay-Time          [41]  6   0
00:03:13: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
h323-disconnect-time=*16:03:11.306 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS:  Vendor, Cisco       [26]  28  VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS:  Acct-Session-Id     [44]  10  "00000000"
00:03:13: RADIUS:  Acct-Input-Octets   [42]  6   0
00:03:13: RADIUS:  Acct-Output-Octets  [43]  6   88000
00:03:13: RADIUS:  Acct-Input-Packets  [47]  6   0
00:03:13: RADIUS:  Acct-Output-Packets [48]  6   550
00:03:13: RADIUS:  Acct-Session-Time   [46]  6   22
00:03:13: RADIUS:  Vendor, Cisco       [26]  30  VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS:  Vendor, Cisco       [26]  35  VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-bytes-
```

The following is sample output from the **debug radius brief** command:

Example:

```
Router# debug radius brief
Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 0 00.0.0.0:0000, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:00 is now connected to 5559000000
00:05:26: RADIUS: Retransmit id 6
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No valid server found. Trying any viable server
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No response for id 7
00:05:31: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 0 0.0.000.0:0000, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 5559000000, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 0 0.0.000.0:0000, Accounting-response, len 20
```

The following example shows **debug radius hex** command output:

Example:

```
Router# debug radius hex
Radius protocol debugging is on
Radius packet hex dump debugging is on
Router#
17:26:52: RADIUS: ustruct sharecount=3
17:26:52: Radius: radius_port_info() success=0 radius_nas_port=1
17:26:52: RADIUS: Initial Transmit ISDN 0:D:00 id 0 00.0.0.0:0000, Accounting-Request,
len 361
17:26:52:         Attribute 4 6 01081D03
17:26:52:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:26:52:         Attribute 61 6 00000000
17:26:52:         Attribute 1 12 34303835323734323036
17:26:52:         Attribute 30 7 3532393831
17:26:52:         Attribute 31 12 34303835323734323036
17:26:52:         Attribute 40 6 00000001
17:26:52:         Attribute 6 6 00000001
17:26:52:         Attribute 26 27 00000009211568333233 2D67772D69643D353330305F34332E
17:26:52:         Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D38463341333136332042343939383030304620302033424537314238
17:26:52:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:26:52:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:26:52:         Attribute 26 56
000000091932683332332D73657475702D74696D653D2A30393A32363A35322E3838302050535420536174204A616E20312032303030
17:26:52:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142 38
:26:52:         Attribute 44 10 3030303030303035
17:26:52:         Attribute 41 6 00000000
17:26:52: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 0000000000
17:26:52: RADIUS: Received from id 10 10.0.0.1:1824, Accounting-response, len 20
17:27:01: RADIUS: ustruct sharecount=3
17:27:01: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:01: RADIUS: Initial Transmit ISDN 0:D:23 id 11 10.0.0.0:1823, Access-Request, len
173
17:27:01:         Attribute 4 6 01081D03
17:27:01:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:01:         Attribute 61 6 00000000
17:27:01:         Attribute 1 8 313233343536
17:27:01:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:01:         Attribute 31 12 34303835323734323036
17:27:01:         Attribute 2 18 C980D8D0E9A061B3D783C61AA6F27214
17:27:01:         Attribute 26 36
00000009011E683332332D6976722D6F75743D7472616E73616374696F6E49443A33
17:27:01: RADIUS: Received from id 11 0.0.000.0:0000, Access-Accept, len 115
17:27:01:         Attribute 6 6 00000001
17:27:01:         Attribute 26 29 0000000965176833323 32D6372656469742D616D6F756E743D3435
17:27:01:         Attribute 26 27 00000009661568333233 2D6372656469742D74696D653D3333
17:27:01:         Attribute 26 26 000000096714683332332D72657475726E2D636F64653D30
17:27:01:         Attribute 25 7 6C6F63616C
17:27:01: RADIUS: saved authorization data for user 61AA0698 at 6215087C
17:27:09: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 5559999999, call
lasted 17 seconds
17:27:09: RADIUS: ustruct sharecount=2
17:27:09: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:09: RADIUS: Sent class "local" at 621508E8 from user 61AA0698
17:27:09: RADIUS: Initial Transmit ISDN 0:D:23 id 12 0.0.000.0:0000, Accounting-Request,
len 776
17:27:09:         Attribute 4 6 01081D03
17:27:09:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:09:         Attribute 61 6 00000000
17:27:09:         Attribute 1 8 313233343536
17:27:09:         Attribute 30 7 3532393831
17:27:09:         Attribute 31 12 34303835323734323036
```

```
17:27:09:         Attribute 40 6 00000002
17:27:09:         Attribute 25 7 6C6F63616C
17:27:09:         Attribute 45 6 00000001
17:27:09:         Attribute 6 6 00000001
17:27:09:         Attribute 26 27 0000000921156833332332D67772D69643D353330305F34332E
17:27:09:         Attribute 26 57
0000000901336833332332D696E636F6D696E672D636F6E662D69643D384633341333136332042343938303030046
20302033424537314238
17:27:09:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:27:09:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:27:09:         Attribute 26 56
0000000919326833332332D73657475702D74696D653D2A30393A32363A35322E3838302050535420536174204A
616E20312032303030
17:27:09:         Attribute 26 58
000000091C34683332332D636F6E6E6563742D74696D653D2A30393A32363A35322E393037205053542053617 4
204A616E20312032303030
17:27:09:         Attribute 26 61
000000091D37683332332D646973636F6E6E6563742D74696D653D2A30393A32373A31302E3133372050535420
536174204A616E20312032303030
17:27:09:         Attribute 26 32
000000091E1A683332332D646973636F6E6E6563742D63617573653D3130
17:27:09:         Attribute 26 28 000000091F16683332332D766F6963652D7175616C6974793D30
17:27:09:         Attribute 26 48
00000009182A683332332D636F6E662D69643D38463334133313633204234393830303046203020334245373142
38
17:27:09:         Attribute 44 10 3030303030303035
17:27:09:         Attribute 42 6 00000000
17:27:09:         Attribute 43 6 00012CA0
17:27:09:         Attribute 47 6 00000000
17:27:09:         Attribute 48 6 000001E1
17:27:09:         Attribute 46 6 00000011
17:27:09:         Attribute 26 30 0000000901187375627363726962657723D526567756C61724C696E65
17:27:09:         Attribute 26 35
00000009011D683332332D6976722D6F75743D5461726966663A556E6B6E6F776E
17:27:09:         Attribute 26 22 000000090110707 2652D62797465732D696E3D30
17:27:09:         Attribute 26 23 00000000901117072652D62797465732D6F75743D30
17:27:09:         Attribute 26 21 00000009010F7072652D70616B732D696E3D30
17:27:09:         Attribute 26 22 00000000901107072652D70616B732D6F75743D30
17:27:09:         Attribute 26 22 0000000901106E61732D72782D73706565643D30
17:27:09:         Attribute 26 22 0000000901106E61732D74782D73706565643D30
17:27:09:         Attribute 41 6 00000000
17:27:09: RADIUS: Received from id 12 10.0.0.1:1824, Accounting-response, len 20
```

Configuration Examples for PPPoE Service Selection

Example PPPoE Service Selection with ATM QoS and Tunneling Services

In the following example, three services are configured: gold-isp-A, silver-isp-A, and isp-xyz. The gold and silver services are forwarded onto the same tunnel, but the ATM PVCs between the LAC and DSLAM is set up with different QoS parameters depending on the level of service chosen. The isp-xyz service offers users access to the services of the xyz Internet service provider.

In this example, the subscriber profile is configured locally on the PPPoE server.

RADIUS Service Profile Configuration

```
gold-isp-A  Password = "cisco", User-Service-type = Outbound-User
        Tunnel-Assignment-Id = nrp1-3,
        Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
        Cisco-Avpair = "atm:peak-cell-rate =2500",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =400"
silver-isp-A  Password = "cisco",  User-Service-type = Outbound-User
        Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
        Cisco:Cisco-Avpair = "atm:peak-cell-rate =1500",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =200"
isp-xyz  Password = "cisco", User-Service-type = Outbound-User
        Cisco-Avpair = "vpdn:tunnel-id=aol",
        Cisco-Avpair = "vpdn:tunnel-type=l2tp",
        Cisco-Avpair = "vpdn:ip-addresses=10.1.1.5",
        Cisco:Cisco-Avpair = "atm:peak-cell-rate =1000",
        Cisco:Cisco-Avpair = "atm:sustainable-cell-rate =150"
```

PPPoE Server Configuration

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default local
!
! Configure the subscriber profile
policy-map type service listA
 pppoe service gold-isp-A
 pppoe service silver-isp-A
 pppoe service isp-xyz
!
! Configure the PPPoE profile
bba-group pppoe group-A
 virtual-template 1
 sessions per-vc limit 5
 service profile listA
! Attach the PPPoE profile to a PVC
interface atm0/0.0
 pvc 2/200
  protocol PPPoE group group-A
!
```

Example PPPoE Service Selection with Tunneling Services

In the following example, PPPoE service selection is used to provide tunneling services only. In this example, the subscriber profile is configured on the RADIUS server.

RADIUS Service Profile Configuration

```
tunnel-to-cust1 Password = "cisco", User-Service-type = Outbound-User
   Tunnel-Assignment-Id = nrp1-3,
   Cisco-Avpair = "vpdn:tunnel-id=nrp1-3",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.4",
tunnel-to-cust2 Password = "cisco", User-Service-type = Outbound-User
   Cisco-Avpair = "vpdn:tunnel-id=xyz",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.5",

tunnel-to-cust3 Password = "cisco", User-Service-type = Outbound-User
   Cisco-Avpair = "vpdn:tunnel-id=aol",
   Cisco-Avpair = "vpdn:tunnel-type=l2tp",
   Cisco-Avpair = "vpdn:ip-addresses=10.1.1.6",
```

RADIUS Subscriber Profile Configuration

```
customer-tunnels Password = "cisco", User-Service-type = Outbound-User
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust1",
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust2",
   Cisco:Cisco-Avpair = "pppoe:service-name=tunnel-to-cust3"
```

PPPoE Server Configuration

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default group radius
!
! Configure the PPPoE profile
bba-group pppoe group-A
 virtual-template 1
 sessions per-vc  5
 service profile customer-tunnels
!
! Attach the PPPoE profile to PVCs
interface atm0/1/0.10
 pvc 2/200
  protocol PPPoE group pppoe-group-A
!
interface atm0/1/0.10
 pvc 3/300
  protocol PPPoE group pppoe-group-A
```

Where to Go Next

- If you want to establish PPPoE sessions limits for sessions on a specific permanent virtual circuit or VLAN configured on an L2TP access concentrator, refer to the "Establishing PPPoE Session Limits per NAS Port" module.
- If you want to enable an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to an LNS or tunnel switch, refer to the "Enabling PPPoE Relay Discovery and Service Selection Functionality" module.
- If you want to configure the transfer upstream of the Point-to-Point Protocol over X (family of encapsulating communications protocols implementing PPP)(PPPoX) session speed value, refer to the "Configuring Upstream Connections Speed Transfer" module.
- If you want to use the Simple Network Management Protocol (SNMP) to monitor PPPoE sessions, refer to the "Monitoring PPPoE Sessions with SNMP" module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, refer to the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, refer to the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

Related Documents

Related Topic	Document Title
RADIUS attributes and configuration	*Cisco IOS XE Security Configuration Guide*, Release 2
Tunneling configuration	*Cisco IOS XE Dial Technologies Configuration Guide* , Release 2
Broadband access aggregation concepts, preparing for broadband access aggregation, and configuring PPPoE sessions	*Cisco IOS XE Broadband Access Aggregation and DSL Configuration Guide*, Release 2
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS XE Broadband Access Aggregation and DSL Command Reference*

Standards

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

MIBs

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

RFCs

RFCs	Title
RFC 2516	A Method for Transmitting PPP over Ethernet (PPPoE), February 1999

Technical Assistance

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

Feature Information for PPPoE Service Selection

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

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

Table 31 Feature Information for PPPoE Service Selection

Feature Name	Releases	Feature Configuration Information
PPPoE Service Selection	Cisco IOS XE Release 2.1	The PPPoE Service Selection feature uses service tags to enable a PPP over Ethernet (PPPoE) server to offer PPPoE clients a selection of services during call setup. You choose one of the services offered, and the service is provided when the PPPoE session becomes active. The following commands were introduced or modified: **service profile**, **pppoe service**, **virtual-template**.