Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS Release 15MT

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

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

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Preparing for Broadband Access Aggregation

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

Additional information can be found in these documents:

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

Restrictions for Preparing for Broadband Access Aggregation

Broadband scalability is not intended to improve the scalability of the following:

- Scaling for dial-out
- Scaling for PPP callback
- Scaling virtual profiles
- Scaling Multilink PPP (MLP)
- Various PPP (PPPoX) applications that terminate PPP on physical interfaces

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 (VPDN), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

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; therefore, multiple PVCs can use a single virtual template.

Cisco IOS software supports up to 200 virtual-template configurations. If greater numbers of tailored configurations are required, an authentication, authorization, and accounting (AAA) server may be employed. Refer to the "Configuring Per-User Configuration" chapter in the Cisco IOS Dial Technologies Configuration Guide for additional information on configuring an AAA server.

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. 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 ATM PVC to ensure that such parameters take effect. Alternatively, if parameters are specified after the ATM PVC has been configured, use the **shutdown** command followed by the **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, they 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.

Autosense for ATM PVCs

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

Note The PPPoA/PPPoE Autosense for ATM PVCs feature is supported on SNAP-encapsulated ATM PVCs only. It is not supported on MUX-encapsulated PVCs.

Virtual Access Interface Precloning

Precloning virtual-access interfaces for PPPoA at the NAS enables the virtual-access interface to be allocated at system start. This functionality significantly reduces the load on the system during call setup. When precloning is used, the virtual-access interface is attached to the session upon receipt of the first session-initiation packet from the client. The virtual-access interface is detached upon termination of the PPP session.

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, page 3
- Virtual Template Compatibility with Subinterfaces, page 4

Virtual Access Subinterfaces

The virtual-template command supports existing features, functions, and configurations. By default, the virtual-template subinterface command is enabled.

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 will be created and cloned for all PPP sessions using that virtual template. If the virtual-template subinterface command is disabled, full virtual-access interfaces will always be created.

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

The ppp multilink and ppp callback accept commands will not necessarily prevent subinterfaces from being created. Often, these commands are present in a virtual-template configuration, but PPP does not negotiate them. If neither of these features is negotiated, virtual-access subinterfaces will be created. If one or both of these features is negotiated, subinterfaces will not be created. The router will automatically determine if subinterfaces will be created depending on how PPP is negotiated on a case-by-case basis.

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.

If the creation of virtual-access subinterfaces is disabled by the no virtual-template subinterface command, the test virtual-template subinterface command produces no output.

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 Using 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 PVCs, page 5
- Configuring a Virtual Template, page 9
- Precloning Virtual-Access Interfaces, page 10
- Configuring Enhancements for Broadband Scalability, page 11

Configuring PVCs

In a digital subscriber line (DSL) environment, many applications require the configuration of a large number of ATM PVCs.

Perform the following tasks to configure PVCs:

Benefits of Configuring a PVC Range

A PVC range saves time because configuring a range of PVCs is faster than configuring a number of PVCs individually.

Using a PVC range saves nonvolatile random access memory (NVRAM) because a range of PVCs takes up less NVRAM on network service routers than a large number of individually configured PVCs.

Using a PVC range speeds boot-up time because the command parser is able to parse one configuration command instead of many.

Configuring an ATM PVC or PVC Range

Perform the following task to configure an ATM PVC or PVC range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* [**point-to-point | multipoint]**
   - or
   - **interface atm** *number.subinterface-number* [**point-to-point | multipoint]**
4. Do one of the following:
   - **pvc** [*name*] *vpi*/*vci*
   - **range** [*range-name*] **pvc** *start-vpi*/*start-vci end-vpi*/*end-vci*
5. exit
6. show atm pvc [*vpi/vci* | **name** | **interface atm** *interface-number*]

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	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* [**point-to-point** | **multipoint]**
	• or
	• **interface atm** *number.subinterface-number* [**point-to-point** | **multipoint]**
	
	Example:
	
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the**interface atm** command.[1]

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi*/*vci*
	• **range** [*range-name*] **pvc** *start-vpi*/*start-vci* *end-vpi*/*end-vci*
	
	Example:
	
	`Router(config-subif)# pvc cisco 0/5`
	
	Example:
	
	`or`
	
	Example:
	
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs.

Step 5	exit **Example:** `Router(config-subif)# exit`	(Optional) Exits the configuration session and returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 6	show atm pvc [*vpi/vci* | **name** | **interface atm** *interface-number*] **Example:** `Router(config)# show atm pvc 0/5`	Displays all ATM permanent virtual connections (PVCs) and traffic information.

Example

The following is sample output from the **show atm pvc** command with the vpi/vci argument specified:

```
Router# show atm pvc 0/41
ATM2/0: VCD: 3, VPI: 0, VCI: 41
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s), OAM retry frequency: 1
second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minutes(s)
InPkts: 31759, OutPkts: 26497, InBytes: 2356434, OutBytes: 1589743
InPRoc: 15785, OutPRoc: 26472, Broadcasts: 0
InFast: 20, OutFast: 20, InAS: 15954, OutAS: 6
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.
```

Configuring an Individual PVC Within a PVC Range

Perform this task to configure an individual 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. **pvc-in-range** [*pvc-name*] [[*vpi*/]*vci*]
6. end
7. show atm pvc [vpi/vci | name | interface atm interface-number]
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	**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 1/100 4/199`	Defines a range of PVCs and enables PVC range configuration mode.
Step 5	**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 PVC-in-range configuration mode.
Step 6	end **Example:** `Router(config-if-atm-range-pvc)# end`	Ends the PVC range configuration mode.
Step 7	show atm pvc [vpi/vci | name | interface atm interface-number] **Example:** `Router(config-if)# show atm pvc pvc1 3/104`	Displays the PVC information.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a Virtual Template

Before configuring the ATM PVC for PPP over ATM, you typically create and configure a virtual template. Use the following commands to create and configure a virtual template.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **encapsulation ppp**
5. **ip unnumbered ethernet** *number*
6. **ppp authentication chap**
7. **no ip route-cache**

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, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Enables PPP encapsulation on the virtual template.
Step 5	**ip unnumbered ethernet** *number* **Example:** `Router(config-if)# ip unnumbered ethernet 1`	(Optional) Enables IP without assigning a specific IP address on the LAN.
Step 6	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	(Optional) Enables CHAP authentication.
Step 7	**no ip route-cache** **Example:** `Router(config-if)# no ip route-cache`	(Optional) Disables IP route-caching.

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. Refer to the "Configuring Virtual Template Interfaces" chapter in the Cisco IOS Dial Technologies Configuration Guide for additional information about configuring the virtual template.

Precloning Virtual-Access Interfaces

Precloning virtual-access interfaces at the NAS reduces the load on the system during call setup. Use the following procedure to preclone a virtual-access interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **virtual-template** *template-number pre-clone number*
4. **show vtemplate**

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	**virtual-template** *template-number pre-clone number* **Example:** `Router(config)# virtual-template 1 pre-clone 250`	Specifies the number of virtual-access interfaces to be created and cloned from a specific virtual access template.
Step 4	**show vtemplate** **Example:** `Router(config-if)# show vtemplate`	Displays the state of virtual-access interface precloning.

Example

In the following sample output, precloning is enabled for Virtual-Template 1, 250 virtual-access interfaces have been precloned, and 249 virtual-access interfaces are available for new PPPoA and PPPoE sessions. Only one virtual-access interface is in use, and no virtual-access interfaces were cloned during call setup.

```
Router# show vtemplate
Virtual-Template 1, pre-cloning is on
 Pre-clone limit: 250, current number: 249
 Active vaccess number: 1
Generic free vaccess number: 0
```

Configuring Enhancements for Broadband Scalability

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

- Verifying Virtual-Template Compatibility with Virtual-Access Subinterfaces, page 11
- Disabling Virtual-Access Subinterfaces, page 12

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.

Example

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
```

Disabling Virtual-Access Subinterfaces

When a virtual template is not compatible with the creation of subinterfaces, use the following task to configure a router to always create full virtual-access interfaces instead of virtual-access subinterfaces.

Note The **virtual-template subinterface** command is enabled by default and does not appear in the running configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no virtual-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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no virtual-template subinterface** **Example:** `Router(config)# no virtual-template subinterface`	Disables the creation of virtual-access subinterfaces. **Note** The **virtual-template subinterface** command is enabled by default.

Configuration Examples for Preparing for Broadband Access Aggregation

ATM PVC Range on a Point-to-Point Subinterface Example

In the following example, a PVC range called "range1" is created with a total of 100 PVCs in the range. A point-to-point subinterface will be created for each PVC in the range. Routed bridge encapsulation is configured on this range.

```
interface atm 6/0.200 point-to-point
 ip unnumbered loopback 1

 atm route-bridged ip
 range range1 pvc 1/200 1/299
 end
```

ATM PVC Range on a Multipoint Subinterface Example

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

```
interface atm 6/0.110 multipoint

 range range-pppoa-1 pvc 100 4/199

 class-range classA

 ubr 1000

 encapsulation aal5snap

 protocol ppp virtual-template 2
```

Individual PVC Within a PVC Range Configuration Example

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

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
 class-range classA
  pvc-in-range pvc1 3/104

 shutdown
```

Virtual-Access Subinterfaces Configuration Examples

This section provides the following configuration examples:

- Virtual-Access Subinterface Configuration Example, page 14
- Testing a Virtual Template for Compatibility with Subinterfaces Example, page 15

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
```

Where to Go Next

To configure broadband access, first select one of the three main configuration tasks:

1. If you want to provide protocol support for PPPoE sessions, refer to the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module. Then go to 2.

or

If you want to provide protocol support for PPP over ATM sessions, refer to the "Providing Protocol support for Broadband Access Aggregation of PPP over ATM Sessions" module. Then go to 2.

or

If you want to provide connectivity from a remote bridged ethernet network to a routed network using ATM routed bridge encapsulation, refer to the "Providing Connectivity Using ATM Routed Bridge Encapsulation" module.

1. If you are using a RADIUS server for access and accounting, refer to the "Identifying the Physical Subscriber Line for RADIUS Access and Accounting" module. Then go to 3.
2. If you are setting up PPPoE services, you can select the following options:

    - 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 control subscriber bandwidth, refer to the "Controlling Subscriber Bandwidth" 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 the transfer upstream of the session speed value, refer to the "Configuring Upstream Connections Speed Transfer" module.

- If you want to use 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

The following sections provide references related to the "Preparing for Broadband Aggregation" module.

Related Documents

Related Topic	Document Title
Configuring a PVC range	"Configuring PVCs" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*
Broadband access aggregation concepts	*" Understanding Broadband Access Aggregation" module of the Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
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*, Release 12.3
Creating a virtual template	"Configuring Virtual Template Interfaces" chapter in the *Cisco IOS Dial Technologies Configuration Guide*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	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
Configuration Enhancements for Broadband Scalability	12.2(13)T 12.2(15)B 12.2(33)SRC	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.

Feature Name	Software Releases	Feature Configuration Information
PPPoA/PPPoE Autosense for ATM PVCs	12.2(4)T 12.2(4)T3	This feature enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

Understanding Broadband Access Aggregation

Broadband access aggregation is the means by which connections are made among multiple technologies. These technologies include ISDN, DSL, cable, Ethernet, and wireless devices that are connected to corporate virtual private networks (VPNs), third-party applications, and the Internet. Subscriber demand for high-speed services, including multi-player gaming, video-on-demand, home security, digital audio, streaming video, and many other applications, require the delivery of IP services, regardless of the access medium.

Because so many different technologies are involved in broadband access aggregation, it is important that the service provider understand their network both in terms of the hardware that makes up the installation, which determines what type of sessions need to be established, but also in terms of what kinds of services their subscribers expect to receive. The demands placed on large service provider installations can often result in the need to contend with millions of sessions and provide flexible and reliable configurations for widely diverse consumer needs.

This module contains conceptual information about broadband access aggregation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Broadband Access Aggregation

Encapsulation Protocols

Internet access has evolved from dialup modems to high-speed broadband. One of the most important considerations in setting up a broadband network is encapsulation. The key protocols include the tunneling protocol and the transport protocol. The tunneled protocol (the one to be encapsulated) gains one or more headers that can be used to identify different tunnels between a pair of devices and ultimately deliver the payload to a remote peer.

Tunneling protocols can be applied to protocols operating at the same layer of the Open Systems Interconnection (OSI) model or at different layers. A wide range of applications can be derived from various tunneling protocols, such as connecting isolated network segments, nondisruptive network renumber, Layer 2 transport, security, and controlling routing behavior.

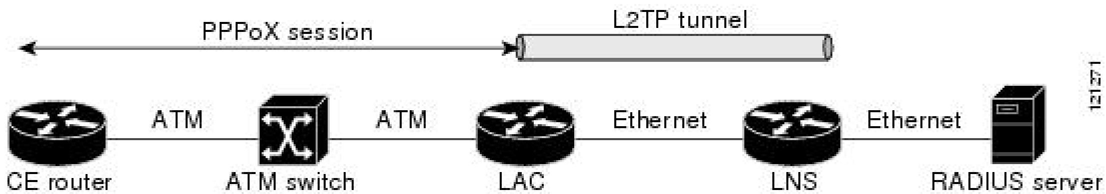
Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is one of the most used building blocks for broadband networks. It is an International Engineering Task Force (IETF) standard that combines aspects of two existing tunneling protocols: Cisco Layer 2 Forwarding (L2F) and Microsoft Point-to-Point Tunneling Protocol (PPTP).

The main component of L2TP is a reliable control channel that is responsible for session setup, negotiation, and teardown, and a forwarding plane that adds negotiated session IDs and forwards traffic. Layer 2 circuits terminate in a device called an L2TP access concentrator (LAC), and the PPP sessions terminate in an L2TP network server (LNS). The LNS authenticates the user and is the endpoint for PPP negotiation.

The LAC connects to the LNS using a LAN or a wide-area network (WAN) switch as a public or private ATM as shown in the figure below. The LAC directs the subscriber session into L2TP tunnels based on the domain of each session. The LAC acts as one side of an L2TP tunnel endpoint and is a peer to the LNS on the other side of the tunnel. The LAC forwards packets to and from the LNS and a remote system.

Figure 1 L2TP Tunnel Between an LAC and an LNS



The LNS is a peer to the LAC and sits on one side of an L2TP tunnel. The LNS routes packets to and from the LAC and a destination network. The broadband aggregation server can be configured to terminate the PPP sessions and route client IP packets onto the ISP network toward their final destination. LNSs can also be configured to place sessions in VRFs before routing the packets.

The following user encapsulations can go into an L2TP tunnel:

- PPP sessions encapsulated in L2TP tunnels (LNS-side support only)
- PPPoE termination over ATM
- PPPoA termination
- PPPoEoE or PPPoEo802.1Q

Cisco’s broadband aggregation routers function as the service provider’s network access server when configured as the LAC. Subscribers can use a local or PPP connection to initiate a PPPoA or PPPoE session to the LAC. The LAC terminates the physical connection and forwards the PPP session to the provider’s LNS.

ATM Services

ATM networks provide the following ATM services, which provide delivery of the subscriber sessions to the service providers access concentrators:

- Permanent virtual circuits (PVC)
- Switched virtual circuits (SVC)

A PVC allows direct connectivity between sites. In this way a PVC is similar to a leased line. PVCs generally guarantee availability of a connection, and no call setup procedures are required between ATM switches. However, PVCs provide a static connectivity and require manual administration to set up.

An SVC is created and released dynamically and remains in use only as long as data is being transferred. In this way it is similar to a telephone call. Dynamic call control requires a signaling protocol between the ATM endpoint and the ATM switch. SVCs provide connection flexibility and call setup that can be automatically handled by a networking device. Setting up the connection requires extra time and overhead.

ATM supports two types of connections:

- Point-to-point
- Point-to-multipoint

A point-to-point ATM connection connects two ATM end systems and can be unidirectional (one-way communication) or bidirectional (two-way communication).

A point-to-multipoint ATM connection connects a single source end-system (known as the Root node) to multiple destination end-systems (known as leaves). Such connections are unidirectional only. Root nodes can transmit to leaves, but leaves cannot transmit to the root or to each other on the same connection.

PPPoE

PPP over Ethernet (PPPoE) provides the ability to connect hosts on a network over a simple bridging device to a remote aggregation concentrator. PPPoE is the predominant access protocol in broadband networks worldwide. PPPoE typically is deployed with a software stack housed on the end-customer’s (subscriber’s) PC. This software allows the network service provider to "own" the customer as the PPP session runs from the customer PC to the service provider network.

PPPoEoE PPPoEo802.1q

PPPoEoE is a variant of PPPoE where the Layer 2 transport protocol is now Ethernet or 802.1q VLAN instead of ATM. This encapsulation method is generally found in Metro Ethernet or Ethernet digital subscriber line access multiplexer (DSLAM) environments. The common deployment model is that this encapsulation method is typically found in multi-tenant buildings or hotels. By delivering Ethernet to the subscriber, the available bandwidth is much more abundant and the ease of further service delivery is increased.

PPPoA

With PPP over ATM (PPPoA), a customer premises equipment (CPE) device encapsulates the PPP session based on RFC 1483 for transport across the DSLAM. PPPoA is commonly used in SOHO and branch office type environments although it is not limited to them. It has greater flexibility for the home than the average PPPoE deployment because the customer LAN behind the CPE is under the complete control of the customer and the CPE acts as a router as opposed to a bridge for PPPoE.

When you configure PPP over ATM, a logical interface known as a virtual access interface associates each PPP connection with an ATM VC. You can create this logical interface by configuring an ATM PVC or SVC. This configuration encapsulates each PPP connection in a separate PVC or SVC, allowing each PPP connection to terminate at the router ATM interface as if received from a typical PPP serial interface.

The virtual access interface for each VC obtains its configuration from a virtual interface template (virtual template) when the VC is created. Before you create the ATM VC, it is recommended that you create and configure a virtual template as described in the "Preparing for Broadband Access Aggregation" module.

Once you have configured the router for PPP over 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.

The virtual access interface remains associated with a VC as long as the VC is configured. If you remove the configuration of the VC, the virtual access interface is marked as deleted. If you shut down the associated ATM interface, you will also cause the virtual access interface to be marked as down (within 10 seconds), and you will bring the PPP connection down. If you set a keepalive timer of the virtual template on the interface, the virtual access interface uses the PPP echo mechanism to verify the existence of the remote peer.

The following three types of PPP over ATM connections are supported:

- IETF-compliant MUX encapsulated PPP over ATM
- IETF-compliant LLC encapsulated PPP over ATM
- Cisco-proprietary PPP over ATM

Routed Bridge Encapsulation

ATM routed bridge encapsulation (RBE) is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

The ATM subinterface on a head-end router is configured to function in ATM routed-bridge encapsulation mode. This configuration is useful when a remote bridged Ethernet network device needs connectivity to a routed network by way of a device bridging from an Ethernet LAN to an ATM RFC 1483 bridged encapsulation.

The bridged ATM interface supports ATM PVCs and ATM SVCs.

Because PVCs are statically configured along the entire path between the end systems, it would not be suitable to route bridged encapsulated traffic over them when the user wants to configure the VCs dynamically and tear down the VCs when there is no traffic.

The Subscriber Service Switch was developed in response to a need by Internet service providers 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.

Cisco Subscriber Service Switch

The Cisco Subscriber Service Switch provides flexibility on where and how many subscribers are connected to available services and how those services are defined. 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, emerging 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 between 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).

As networks grow beyond the campus, network security increases in importance and administration complexity. Customers need to protect networks and network resources from unauthorized access by remote users. Cisco Systems uses a strategy known as authentication, authorization, and accounting (AAA) for verifying the identity of, granting access to, and tracking the actions of remote users. In today’s networks, the TACACS+ and RADIUS protocols are commonly used to provide AAA solutions. Support for RADIUS along with TACACS+ enables Cisco to deliver tremendous flexibility and choice to organizations in AAA functionality.

RADIUS Support in Cisco IOS

Cisco Systems introduced support for RADIUS in Cisco IOS Release 11.1 in its network access server (NAS) devices.

The RADIUS protocol is an access server authentication and accounting protocol. RADIUS has gained support among a wide customer base, including Internet service providers (ISPs).

The RADIUS protocol is based on a client/server model. An NAS operates as a client of RADIUS. The client is responsible for passing user information to a designated RADIUS server and then acting on the response that is returned.

A RADIUS server (or daemon) can provide authentication and accounting services to one or more client NAS devices. RADIUS servers are responsible for receiving user connection requests, authenticating users, and then returning all configuration information necessary for the client to deliver service to the users. A RADIUS access server is generally a dedicated workstation connected to the network.

Additional References

Related Documents

Related Topic	Document Title
Configuring a PVC range	"Configuring PVCs" in the Cisco IOS Wide-Area Networking Configuration Guide
Creating a virtual template	"Configuring Virtual Template Interfaces" chapter in the Cisco IOS Dial Technologies Configuration Guide

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

ABR --available bit rate. QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data.

ACR --allowed cell rate. A parameter defined by the ATM Forum for ATM traffic management. ACR varies between the MCR and the PCR, and is controlled dynamically using congestion control mechanisms.

CBR --constant bit rate. QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.

MCR --minimum cell rate. Parameter defined by the ATM Forum for ATM traffic management. MCR is defined only for ABR transmissions, and specifies the minimum value for the ACR.

NAS --network access server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

PCR --peak cell rate. Parameter defined by the ATM Forum for ATM traffic management. In Constant Bit Rate (CBR) transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR.

PPP --Point-to-Point Protocol. PPP is the successor to Serial Line Internet Protocol (SLIP) that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: Link Control Protocol (LCP) and Network Control Protocol (NCP).

PPPoA --Point-to-Point Protocol over ATM. The PPPoA feature enables a high-capacity central site router with an Asynchronous Transfer Mode (ATM) interface to terminate multiple remote Point-to-Point Protocol (PPP) connections.

PPPoE --Point-to-Point Protocol over Ethernet. PPPoE allows a PPP session to be initiated on a simple bridging Ethernet connected client.

PPPoX --Point-to-Point Protocol over Protocol. PPPoX indicates that the point-to-point protocol terminates on another protocol which could be ATM or Ethernet.

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

QoS --quality of service. Cisco IOS QoS technology lets complex networks control and predictably service a variety of networked applications and traffic types.

RADIUS--Remote Authentication Dial-in User Service

SCR--sustainable cell rate. Parameter defined by the ATM Forum for ATM traffic management. For VBR connections, SCR determines the long-term average cell rate that can be transmitted.

UBR--unspecified bit rate. QoS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network but there are no guarantees in terms of cell loss rate and delay.

VBR--variable bit rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (rt) class and non-real time (nrt) class. VBR (rt) is used for connections in which there is a fixed timing relationship between samples. VBR (nrt) is used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS.

VPDN--virtual private dialup network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost effective method of establishing a long distance, point-to-point connection between remote dial users and a private network.

VSA--vendor-specific attribute. An 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.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

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

- You must understand the concepts described in the "Understanding Broadband Access Aggregation" module.
- Optionally you may perform the preparation tasks in the "Preparing for Broadband Access Aggregation" module

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

PPP over ATM cannot be configured on IETF-compliant Logical Link Control (LLC) encapsulated PPP over ATM.

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

PPP over ATM Configuration Scenario

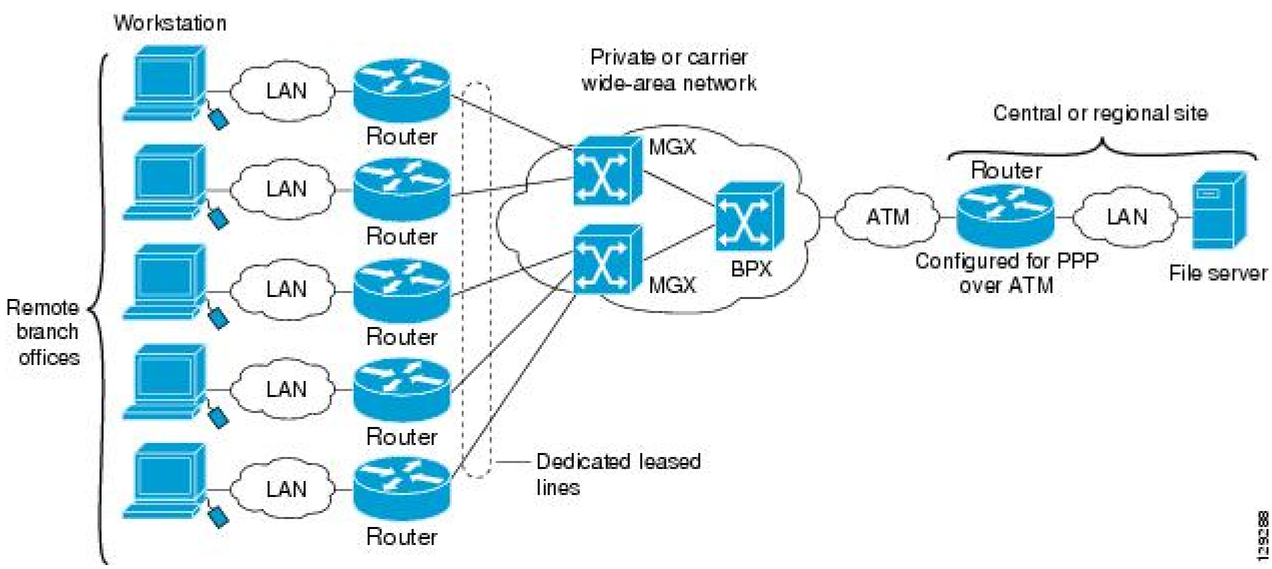
PPP over ATM can be configured on all platforms running Cisco IOS Release 12.1 or later.

Note

All forms of PPP over ATM are supported on the ATM port adapters, except for the PA-A1 ATM port adapter for Cisco IOS Release 12.1. All forms of PPP over ATM are now supported on the enhanced ATM port adapter for Cisco IOS Release 12.1 or later.

The figure below shows a typical scenario for using Cisco-proprietary PPP over ATM.

Figure 2 PPP-over-ATM Network Environment



Note If you need to configure the Cisco MGX 8220 shelf for frame forwarding at the remote sites, refer to the Cisco MGX 8220 Command Supplement for command line instructions or the Cisco StrataView Plus Operations Guide for StrataView Plus instructions. If you configure the MGX using the command line interface, use the **addport** and **addchan** commands and select frame forwarding for the *port-type* and *chan-type* arguments, respectively.

Virtual Access Interface

When you configure PPP over ATM, a logical interface known as a *virtual access interface* associates each PPP connection with an ATM VC. You can create this logical interface by configuring an ATM permanent virtual circuit (PVC) or switched virtual circuit (SVC). This configuration encapsulates each PPP connection in a separate PVC or SVC, allowing each PPP connection to terminate at the router ATM interface as if received from a typical PPP serial interface.

The virtual access interface for each virtual circuit (VC) obtains its configuration from a virtual interface template (virtual template) when the VC is created. Before you create the ATM VC, it is recommended that you create and configure a virtual template as described in the "Preparing for Broadband Access Aggregation" module.

Once you have configured the router for PPP over 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.

The virtual access interface is associated with the VC after LCP negotiation completes. When the PPP session goes down, the virtual access interface is no longer associated with the VC and is returned to the pool of free virtual-access interfaces.

If you set a keepalive timer of the virtual template on the interface, the virtual access interface uses the PPP echo mechanism to verify the existence of the remote peer.

The following three types of PPP over ATM connections are supported:

- IETF-compliant MUX encapsulated PPP over ATM
- IETF-compliant LLC encapsulated PPP over ATM
- Cisco-proprietary PPP over ATM

Autosense for ATM PVCs

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

Note The PPPoA/PPPoE autosense for ATM PVCs feature is supported on SNAP-encapsulated ATM PVCs only. It is not supported on MUX-encapsulated PVCs.

- Benefits of Autosense for ATM PVCs, page 31

Benefits of Autosense for ATM PVCs

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

How to Provide Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Configuring IETF-Compliant MUX Encapsulated PPP over ATM

Internet Engineering Task Force (IETF)-compliant multiplexer (MUX) encapsulated PPP over ATM, also known as null encapsulation, allows you to configure PPP over ATM using a VC multiplexed encapsulation mode. This feature complies with IETF RFC 2364 entitled PPP over AAL5.

You can configure ATM PVCs for IETF-compliant MUX encapsulated PPP over ATM on either point-to-point or multipoint subinterfaces. Multiple PVCs on multipoint subinterfaces significantly increase the maximum number of PPP-over-ATM sessions running on a router. You can configure IETF-compliant MUX encapsulated PPP over ATM over a single ATM PVC or an ATM PVC range.

IETF-compliant PPP over ATM is not supported on ATM SVCs and can only be applied to PVCs.

The IETF-compliant PPP over ATM feature was designed to support installations with AppleTalk Data Stream Protocol (ADSL) circuits. For an example of using ADSL termination, see the ADSL Termination Example, page 54.

Perform this task to configure IETF-compliant MUX Encapsulated PPP over ATM.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* **point-to-point**
   -
   - or
   - **interface atm** *number.subinterface-number* **point-to-point**
   -
   -
   - **interface atm** *slot/port.subinterface-number* **multipoint**
   -
   -
   - **interface atm** *number.subinterface-number* **multipoint**
4. Do one of the following:
   - **pvc** [*name*] *vpi* **/** *vci*
   -
   -
   - **range** [*range-name*] **pvc** *start-vpi* **/** *start-vci end-vpi* **/** *end-vci*
5. **encapsulation aal5mux ppp virtual-template** *number*

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	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	•
	• or
	• **interface atm** *number.subinterface-number* **point-to-point**
	•
	•
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	•
	•
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	Example:
	
	Example:
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[2]

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

	Command or Action	Purpose

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	•
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	
	Example:
	`Router(config-subif)# pvc cisco 0/5`
	
	Example:
	
	Example:
	`or`
	
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs.

Step 5	**encapsulation aal5mux ppp virtual-template** *number*
	
	Example:
	`Router(config-subif-atm-vc)# encapsulation aal5mux ppp virtual-template 3`
	
	Example:
	`or`
	
	Example:
	`Router(config-subif-atm-range) encapsulation aal5mux ppp virtual-template 3`
		Configures VC multiplexed encapsulation on a PVC or PVC range.

Configuring IETF-Compliant LLC Encapsulated PPP over ATM

IETF-compliant LLC encapsulated PPP over ATM allows you to configure PPP over ATM with LLC encapsulation. It accommodates Frame Relay-to-ATM service interworking (Frame Relay Forum standard FRF.8). There is no equivalent VC multiplexed encapsulation mode for Frame Relay; therefore, LLC encapsulation is required for Frame Relay-to-ATM networking. This version of PPP over ATM also enables you to carry multiprotocol traffic. For example, a VC will carry both PPP and IPX traffic.

The figure below shows Frame Relay-to-ATM interworking.

Figure 3 *Frame Relay-to-ATM Interworking*

You can configure ATM PVCs for IETF-compliant LLC encapsulated PPP over ATM on either point-to-point or multipoint subinterfaces. Multiple PVCs on multipoint subinterfaces significantly increase the maximum number of PPP-over-ATM sessions running on a router.

You can also configure IETF-compliant LLC encapsulated PPP over ATM in a VC class and apply this VC class to an ATM VC, subinterface, or interface. For information about configuring a VC class, refer to the section "Configuring VC Classes" in the module "Configuring ATM."

Note Depending on whether you configure IETF-compliant LLC encapsulated PPP over ATM directly on a PVC or interface, your PVC will inherit the configuration that takes highest precedence. For a description of the inheritance hierarchy, see the **protocol** command in the Cisco IOS Wide-Area Networking Command Reference Guide.

Perform this task to configure IETF-compliant LLC encapsulated PPP over ATM on a PVC or range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* **point-to-point**
   - or
   - **interface atm** *number.subinterface-number* **point-to-point**
   - **interface atm** *slot/port.subinterface-number* **multipoint**
   - or
   - **interface atm** *number.subinterface-number* **multipoint**
4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi*/*end-vci*
5. **encapsulation aal15snap**
6. protocol ppp virtual-template *number*

DETAILED STEPS

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

Step 3	Do one of the following:
	
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	• or
	• **interface atm** *number.subinterface-number* **point-to-point**
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	• or
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[3]

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

	Command or Action	Purpose

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi*/*end-vci*
	
	Example:
	`Router(config-subif)# pvc cisco 0/5`
	
	Example:
	`or`
	
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs.

Step 5	**encapsulation aal15snap** **Example:** `Router(config-subif-atm-vc)#` **encapsulation aal15snap** **Example:** `or` **Example:** `Router(config-subif-atm-range)#` **encapsulation aal15snap**	Configures LLC SNAP encapsulation on the PVC or range of PVCs.[4]

4 "SNAP encapsulation" is a misnomer here, since this encapsulation configures both LLC and SNAP encapsulation on the VC. If SNAP encapsulation is not configured at a lower inheritance level, or another type of encapsulation is configured at a lower inheritance level, you will have to configure both SNAP and the protocol ppp command to ensure that PPP over ATM with LLC encapsulation is configured on your VC.

	Command or Action	Purpose

Step 6	protocol ppp virtual-template *number*
	
	Example:
	
	`Router(config-subif-atm-vc)# protocol ppp virtual-template 2`
	
	Example:
	
	`or`
	
	Example:
	
	`Router(config-subif-atm-range)# protocol ppp virtual-template 2`
		Configures IETF PPP over ATM LLC encapsulation on the PVC or range of PVCs.

Configuring Cisco-Proprietary PPP over ATM PVCs

You can configure ATM PVCs for Cisco-proprietary PPP over ATM on either point-to-point or multipoint subinterfaces. Configuring multiple PVCs on multiple subinterfaces significantly increases the maximum number of PPP-over-ATM sessions running on a router. Remote branch offices must have Cisco-proprietary PPP over ATM configured on PPP-compatible devices interconnecting directly to Cisco's ATM Switch Interface Shelf (AXIS) equipment through a leased-line connection. The shelves provide frame forwarding encapsulation and are terminated on BPX cores prior to connecting to a Cisco 7500 series router.

Perform this task to configure Cisco-proprietary PPP over ATM on a PVC or range of PVCs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* **point-to-point**
   -
   - or
   - **interface atm number .** *subinterface-number* **point-to-point**
   -
   -
   - **interface atm** *slot/port.subinterface-number* **multipoint**
   -
   -
   - **interface atm** *number.subinterface-number* **multipoint**
4. Do one of the following:
   - **pvc** [*name*] *vpi* / *vci*
   -
   -
   - **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **encapsulation aal5ciscoppp virtual-template** *number*

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	•
	• or
	• **interface atm number .** *subinterface-number* **point-to-point**
	•
	•
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	•
	•
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	Example:
	
	Example:
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[5]

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

	Command or Action	Purpose

Step 4	Do one of the following:
	• **pvc** [*name*] *vpi* / *vci*
	•
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	
	Example:
	`Router(config-subif)# pvc cisco 0/5`
	
	Example:
	
	Example:
	`or`
	
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures the PVC or a range of PVCs.

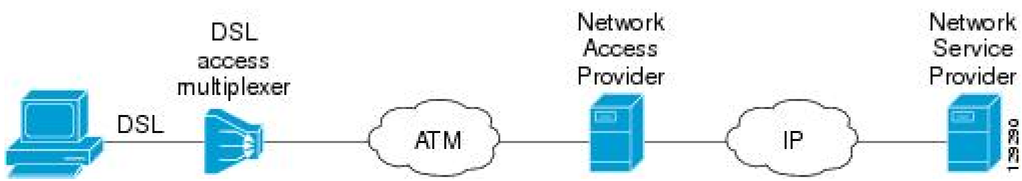
Step 5	**encapsulation aal5ciscoppp virtual-template** *number*
	
	Example:
	`Router(config-subif-atm-vc)# encapsulation aal5ciscoppp virtual-template 4`
	
	Example:
	
	Example:
	`or`
	
	Example:
	`Router(config-subif-atm-range)# encapsulation aal5ciscoppp virtual-template 3`
		Configures Cisco-proprietary PPP over ATM encapsulation on a PVC or PVC range.

Configuring SVCs for NAPs and NSPs

When PPP over ATM is configured over an SVC rather than a PVC, an ATM SVC is established using a configured ATM address each time an end user initiates a connection to a Network Access Provider (NAP) or Network Service Provider (NSP). A PPP session is then established over the SVC. By using PPP, the NAPs and NSPs can authenticate users and provide suitable access to the various services being offered. Whereas PVCs require that services and destination addresses be predetermined, using PPP over ATM SVCs allows users to choose services and the quality of those services dynamically on the basis of the destination address.

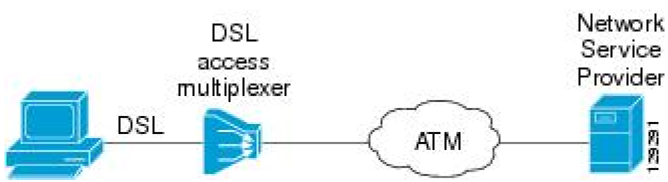
The figure below shows a typical network topology for PPP over ATM SVCs terminating at an NAP.

Figure 4 PPP over ATM SVC Terminating at a Network Access Provider



The figure below shows a typical network topology of PPP over ATM SVCs terminating at an NSP.

Figure 5 PPP over ATM SVC Terminating at a Network Service Provider



The PPP over ATM SVCs feature works by associating each PPP session with a virtual-access interface. Each virtual-access interface is associated with an SVC. The SVCs use static maps that hold information about the encapsulation type and virtual template number. A single static map can accept multiple PPP over ATM SVC calls.

Perform this task to configure PPP over an ATM SVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
    - **interface atm** *slot/port.subinterface-number* **point-to-point**
    -
    - or
    - **interface atm** *number.subinterface-number* **point-to-point**
    -
    -
    - **interface atm** *slot/port.subinterface-number* **multipoint**
    -
    -
    - **interface atm** *number.subinterface-number* **multipoint**
4. **svc** [*name*]
5. **encapsulation aal5auto**
6. **protocol ppp virtual-template** *number*
7. **max vc** *number*
8. **max bandwidth** *kbps*
9. **exit**
10. **exit**
11. **atm nsap-address** *nsap-address*
12. exit
13. **show atm svc**
14. **show atm svc ppp**

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	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	•
	• or
	• **interface atm** *number.subinterface-number* **point-to-point**
	•
	•
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	•
	•
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	Example:
	
	Example:
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[6]

Step 4	**svc** [*name*] **Example:** `Router(config-subif)# svc cisco`	Configures the SVC.
Step 5	**encapsulation aal5auto** **Example:** `Router(config-subif-atm-vc)# encapsulation aal5auto`	Specifies encapsulation auto, which allows the SVC to use either aal5snap or aal5mux encapsulation types.

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

	Command or Action	Purpose
Step 6	**protocol ppp virtual-template** *number* **Example:** `Router(config-subif-atm-vc)# protocol ppp virtual-template 6`	Specifies that PPP is established over the ATM SVC using the configuration from the specified virtual template.
Step 7	**max vc** *number* **Example:** `Router(config-subif-atm-vc)# max vc 5`	Specifies the maximum number of SVCs that can be established using the current configuration.
Step 8	**max bandwidth** *kbps* **Example:** `Router(config-subif-atm-vc)# max bandwidth 564`	Specifies the total amount of bandwidth available to all SVCs in the current configuration.
Step 9	**exit** **Example:** `Router(config-subif-atm-vc)# exit`	Exits VC configuration mode and returns to subinterface configuration mode.
Step 10	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode and returns to interface configuration mode.

Step 11	**atm nsap-address** *nsap-address*
	
	Example:
	
	`Router(config)#`
	`atm nsap-address AB.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12`
		Sets the network service access point (NSAP) address for the ATM interface.

Step 12	exit **Example:** `Router(config)# exit`	Exits configuration mode and returns to EXEC command mode.

	Command or Action	Purpose
Step 13	**show atm svc** **Example:** `Router# show atm svc`	Displays all ATM SVCs and traffic information.
Step 14	**show atm svc ppp** **Example:** `Router# show atm svc ppp`	Displays information about each SVC configured for PPP over ATM.

Configuring PPPoA Autosense for a Single PVC

Perform the following task to configure PPPoA/PPPoE autosense on a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* **point-to-point**
   -
   - or
   - **interface atm number .** *subinterface-number* **point-to-point**
   -
   -
   - **interface atm** *slot/port.subinterface-number* **multipoint**
   -
   -
   - **interface atm** *number.subinterface-number* **multipoint**
4. **pvc** [*name*] *vpi/vci*
5. **encapsulation aal5autoppp virtual-template** *number*

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	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	•
	• or
	• **interface atm number .** *subinterface-number* **point-to-point**
	•
	•
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	•
	•
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	Example:
	
	Example:
	
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[7]

Step 4	**pvc** [*name*] *vpi*/*vci* **Example:** `Router(config-subif)# pvc cisco 0/5`	Configures the PVC.

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

	Command or Action	Purpose
Step 5	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-subif-atm-vc)# encapsulation aal5ciscoppp virtual-template 1`	Configures PPPoA/PPPoE autosense. Also specifies the virtual template interface to use to clone the new virtual-access interface for PPP session on this PVC.

Configuring PPPoA Autosense for a VC Class

Use the following procedure to configure PPPoA/PPPoE autosense on a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation aal5autoppp virtual-template** *number*
5. **exit**
6. Do one of the following:
   - **interface atm** *slot/port.subinterface-number* **point-to-point**
   -
   - or
   - **interface atm** *number* **.** *subinterface-number* **point-to-point**
   -
   -
   - **interface atm** *slot/port.subinterface-number* **multipoint**
   -
   -
   - **interface atm** *number.subinterface-number* **multipoint**
7. **class-int** *vc-class-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	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm class3`	Creates and names a map class.
Step 4	**encapsulation aal5autoppp virtual-template** *number* **Example:** `Router(config-vc-class)# encapsulation aal5ciscoppp virtual-template 1`	Configures PPPoA/PPPoE autosense. Also specifies the virtual template interface to use to clone the new virtual-access interface for PPP session on this PVC.
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Returns to global configuration mode.

	Command or Action	Purpose

Step 6	Do one of the following:
	• **interface atm** *slot/port.subinterface-number* **point-to-point**
	•
	• or
	• **interface atm** *number* **.** *subinterface-number* **point-to-point**
	•
	•
	• **interface atm** *slot/port.subinterface-number* **multipoint**
	•
	•
	• **interface atm** *number.subinterface-number* **multipoint**
	
	Example:
	`Router(config)# interface atm 6/0.200 point-to-point`
	
	Example:
	
	Example:
	
	Example:
	`Router(config)# interface atm 1/0/0.4 multipoint`
		Specifies the ATM point-to-point or multipoint subinterface using the appropriate format of the **interface atm** command.[8]

Step 7	**class-int** *vc-class-name* **Example:** `Router(config-subif)# class-int class3`	Applies the VC class to all VCs on the ATM interface or subinterface.

Verifying PPPoA Autosense for ATM PVCs

Use the following procedure to verify PPPoA/PPPoE autosense.

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show atm pvc** [**ppp**]

After the client at the other end of the PVC has initiated a PPPoA session, use this command to check that the PVC contains the PPPoA session.

Step 2 **show caller**

Use this command to:

- View individual users and consumed resources on the NAS.
- Inspect active call statistics for large pools of connections. (The **debug** commands produce too much output and tax the CPU too heavily.)
- Display the absolute and idle times for each user. The current values for both of these settings are displayed on the TTY line and the asynchronous interface. Users that have been idle for unacceptably long periods of time can be easily identified. By using this information, you can define time-out policies and multiple grades of services for different users.

Example:

```
Router# show caller
Line      User                  Service       Active
  con 0     -                     TTY           00:08:21
  BR0:1     hatteras              PPP           00:00:14
  Vi1       hatteras              PPP   Bundle  00:00:13
```

Step 3 **show interface virtual access** *number*

Displays information about the virtual-access interface, link control protocol (LCP), protocol states, and interface statistics:

Example:

```
Router# show interface virtual access Virtual-Access3
Virtual-Access3 is up, line protocol is up
```

Step 4 **show user**

Displays information about the active lines on the router.

Example:

```
Router# show user

Line User Host(s) Idle Location * 2 vty 0 idle 00:00:00 bru-cse-058.cisco.com tty 2/01 ww Async
interface 00:00:01 PPP: 12.12.12.3
```

Step 5 **show vpdn**

Displays information about active Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a virtual private dial-up network (VPDN).

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
```

Configuration Examples for Configuring PPP over ATM

IETF-Compliant MUX Encapsulated PPP over ATM Configuration Examples

This section provides the following examples for configuring IETF-compliant PPP over ATM:

IETF-Compliant PPP over ATM with Different Traffic-Shaping Parameters Example

PVCs with different PPP-over-ATM traffic-shaping parameters can be configured on the same subinterface. In the following example, three PVCs are configured for PPP over ATM on subinterface ATM 2/0.1. PVC 0/60 is configured with IETF-compliant PPP over ATM encapsulation. Its traffic-shaping parameter is an unspecified bit rate with peak cell rate at 500 kbps. PVC 0/70 is also configured with IETF-compliant PPP over ATM encapsulation, but its traffic-shaping parameter is nonreal-time variable bit rate, with peak cell rate at 1 Mbps, sustainable cell rate at 500 kbps, and burst cell size of 64 cells. PVC 0/80 is configured with the Cisco-proprietary PPP over ATM encapsulation. Its traffic-shaping parameter is an unspecified bit rate with peak cell rate at 700 kbps. For further information, refer to the Configuring IETF-Compliant MUX Encapsulated PPP over ATM, page 32 earlier in this module.

```
interface atm 2/0.1 multipoint
 pvc 0/60
```

```
  encapsulation aal5mux ppp virtual-template 3
   ubr 500
  exit

pvc 0/70
 encapsulation aal5mux ppp virtual-template 3
 vbr-nrt 1000 500 64
  exit
pvc 0/80
 encapsulation aal5ciscoppp virtual-template 3
 ubr 700
 exit
```

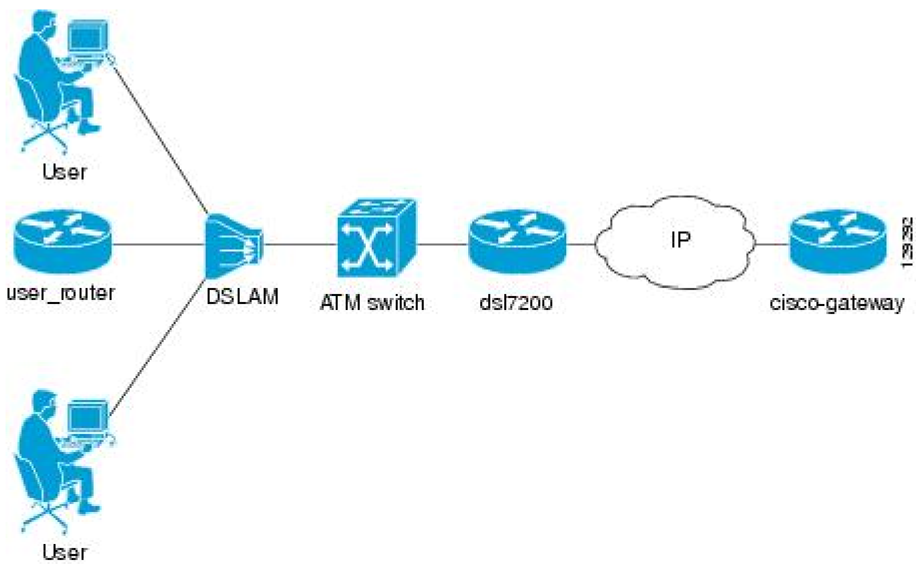
ADSL Termination Example

The IETF-Compliant PPP over ATM feature was designed to support installations with asymmetric digital subscriber line (ADSL) circuits. The figure below illustrates a topology for ADSL termination. This topology allows you to establish a PPP connection to a Cisco 7200 series router.

The example also illustrates the use of PPP tunneling using L2TP to provide VPDN services, in this case for the domain cisco.com. Thus, a user who logs in as bob2257@cisco.com is automatically tunneled to IP address 10.1.2.3. (See the module "Configuring Virtual Private Networks" in the *Cisco IOS VPDN Configuration Guide* for details about setting up VPDN services.)

An example of the commands that you might enter for the user_router, dsl7200, and cisco-gateway (as shown in the figure below) are described below. For further information, refer to the Configuring IETF-Compliant MUX Encapsulated PPP over ATM, page 32 earlier in this module.

Figure 6 ADSL Termination



user_router Configuration

```
interface virtual-template 1
ip address negotiated
ppp chap hostname user_router@cisco.com
ppp chap password 0 cisco
exit

interface atm 0
```

```
pvc 0/40
encapsulation aal5mux ppp virtual-template 1
exit
exit
```

dsl7200 Configuration

```
username user_router@cisco.com password 0 cisco
username dsl7200 password 0 cisco
vpdn enable
vpdn-group 1
request dialin l2tp ip 10.2.1.1 domain cisco.com
interface virtual-template 1
ppp authentication chap
exit
interface atm 2/0
pvc 0/40
encapsulation aal5mux ppp virtual-template 1
exit
exit
```

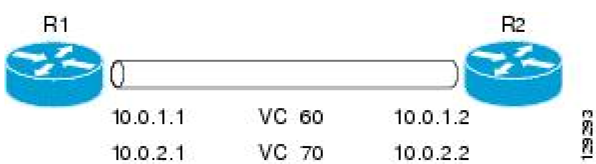
cisco-gateway Configuration

```
username cisco_gateway password 0 cisco
username user_router@cisco.com password 0 cisco
vpdn enable
vpdn-group 1
accept dialin l2tp virtual-template 1 remote dsl7200
interface loopback 0
ip address 10.0.1.1 255.255.255.0
exit
interface virtual-template 1
ip unnumbered loopback 0
peer default ip address pool pool-1
exit
ip local pool pool-1 10.1.2.1 10.1.2.254
```

Two Routers with Back-to-Back PVCs Example

The figure below illustrates an ATM interface with two PPP sessions over two PVC session connections. (See the module "PPP Configuration" in the *Cisco IOS Dial Technologies Configuration Guide* for details on PPP configuration.) The sample commands following the figure below establish the back-to-back router configuration. For further information, refer to the Configuring IETF-Compliant MUX Encapsulated PPP over ATM, page 32 earlier in this module.

Figure 7 Two Routers with Back-to-Back PVCs



R1 Configuration

```
interface atm 2/0
atm clock internal
pvc 0/60
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
```

```
pvc 0/70
encapsulation aal5mux ppp virtual-template 2
vbr-nrt 90 50 1024
exit
interface virtual-template 1
ip address 10.0.1.1 255.255.255.0
interface virtual-template 2
ip address 10.0.2.1 255.255.255.0
exit
```

R2 Configuration

```
interface atm 2/0.1 multipoint
pvc 0/60
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
pvc 0/70
encapsulation aal5mux ppp virtual-template 2
vbr-nrt 90 50 1024
exit
exit
interface virtual-template 1
ip address 10.0.1.2 255.255.255.0
exit
interface virtual-template 2
ip address 10.0.2.2 255.255.255.0
```

Multiplexed Encapsulation Using VC Class Example

In the following example, PVC 0/60 is configured on subinterface ATM 2/0.1 with a VC class attached to it. For details on creating and applying a VC class, see the section "Configuring VC Classes" in the module "Configuring ATM." By rule of inheritance, PVC 0/60 runs with IETF-compliant PPP over ATM encapsulation using the configuration from interface virtual-template 1. Its parameter is an unspecified bit rate with peak cell at 90 kbps.

```
interface atm 2/0.1
pvc 0/60
class-vc pvc-ppp
exit
exit
vc-class atm pvc-ppp
encapsulation aal5mux ppp virtual-template 1
ubr 90
exit
```

IETF-Compliant LLC Encapsulated PPP over ATM Configuration Examples

This section provides the following examples for configuring IETF-compliant LLC encapsulated PPP over ATM:

- Configuring IETF-Compliant PPP over ATM LLC Encapsulation Example, page 56
- Overriding a Virtual Template for IETF-Compliant PPP over ATM Example, page 57
- Disabling IETF-Compliant PPP over ATM LLC Encapsulation on a Specific VC Example, page 57

Configuring IETF-Compliant PPP over ATM LLC Encapsulation Example

This example shows how to configure IETF PPP over ATM LLC encapsulation in the VC class called ppp-default. The VC class specifies virtual template 1 from which to spawn PPP interfaces, SNAP encapsulation (the default), and a UBR class traffic type at 256 kbps. When the VC class ppp-default is configured on interface 0.1, PVC 0/70 inherits these properties. PVC 0/80 overrides virtual template 1 in the VC class and uses virtual template 2 instead. PVC 0/90 also overrides virtual template 1 and uses virtual template 3 instead. In addition, PVC 0/90 uses a VC multiplexed encapsulation and a UBR class traffic type at 500 kbps. For further information, refer to the IETF-Compliant LLC Encapsulated PPP over ATM Configuration Examples, page 56.

```
interface atm 0.1 multipoint
class-int ppp-default
!
pvc 0/70
exit
!
pvc 0/80
protocol ppp virtual-template 2
exit
!
pvc 0/90
encapsulation aal5mux ppp virtual-template 3
ubr 500
exit
exit
!
vc-class atm ppp-default
protocol ppp virtual-template 1
ubr 256
exit
```

Overriding a Virtual Template for IETF-Compliant PPP over ATM Example

This example illustrates how to use inheritance to override a virtual template configuration for muxppp or ciscoppp encapsulation options. For PVC 5/505, since the encapsulation option at that level is ciscoppp virtual template 1, as specified in the VC class called muxppp, the **protocol ppp virtual-template 2** command overrides only the virtual-template configuration. For further information, refer to the IETF-Compliant LLC Encapsulated PPP over ATM Configuration Examples, page 56.

```
interface atm 2/0
class-int muxppp
!
pvc 5/505
protocol ppp virtual-template 2
exit
!
muxppp
encapsulation aal5ciscoppp virtual-template 1
exit
```

Disabling IETF-Compliant PPP over ATM LLC Encapsulation on a Specific VC Example

This example shows how to limit the configuration of a particular LLC encapsulated protocol to a particular VC. First, we see that the VC class called "ppp" is configured with IETF PPP over ATM with LLC encapsulation and virtual template 1. This VC class is then applied to ATM interface 1/0/0. By configuring SNAP encapsulation by itself on PVC 0/32, you disable IETF PPP over ATM with LLC encapsulation on this particular PVC; PVC 0/32 will only carry IP. For further information, refer to the IETF-Compliant LLC Encapsulated PPP over ATM Configuration Examples, page 56.

```
interface atm 1/0/0
class-int ppp
exit
!
interface atm 1/0/0.100 point-to-point
description IP only VC
ip address 10.1.1.1 255.255.255.0
pvc 0/32
encapsulation aal5snap
```

```
exit
exit
!
vc-class atm ppp
encapsulation aal5snap
protocol ppp virtual-template 1
exit
```

Cisco Proprietary-PPP-over-ATM Example

The following example shows how to configure Cisco-proprietary PPP over ATM to use PPP unnumbered link and Challenge Handshake Authentication Protocol (CHAP) authentication. For further information, refer to the Configuring Cisco-Proprietary PPP over ATM PVCs, page 39.

```
configure terminal
!
interface virtual-template 2
 encapsulation ppp
 ip unnumbered ethernet 0/0
 ppp authentication chap
!
interface atm 2/0.2 point-to-point
 pvc 0/34
 encapsulation aal5ciscoppp virtual-template 2
 exit
```

PPP over an ATM SVC Configuration Example

In the following example, ATM interface 2/0/0 is configured to accept ATM SVC calls whose called party address is 47.0091810000000000400B0A2501.0060837B4740.00. The same ATM NSAP address can be configured on other physical ATM interfaces as well. When a PPP session is established, a virtual-access interface is created and cloned with the configuration from virtual template 1. All PPP sessions established on this ATM interface will use the IP address of loopback interface 0. A maximum of 100 SVCs can be established using this configuration. SVCs established using this configuration cannot take up more than 50 Mbps in total bandwidth.

```
interface ATM 2/0/0
 svc anna
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max vc 100
  max bandwidth 50000
 atm nsap 47.0091810000000000400B0A2501.0060837B4740.00
!
interface virtual-template 1
 ip unnumbered loopback 0
!
interface loopback 0
 ip address 10.7.1.1 255.255.255.0
```

PPPoA PPPoE Autosense on an ATM PVC Example

In the following example, the NAS is configured with PPPoA/PPPoE autosense for ATM PVCs on PVC 30/33:

```
!
! Configure PPP Autosense
!
interface ATM 0/0/0.33 multipoint
 pvc 30/33
  encapsulation aal5autoppp Virtual-Template1
!
```

```
! Configure PPPoE
!
vpdn enable
vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
!
ip cef
interface virtual-template 1
 ip unnumbered fastethernet 0/0/0
 ip route-cache cef
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
```

PPPoA PPPoE Autosense on a VC Class Example

In the following example, the NAS is configured with PPPoA/PPPoE autosense on the VC class called MyClass. MyClass applies PPPoA/PPPoE autosense to all PVCs on the ATM 0/0/0.99 interface.

```
!
! Configure PPP Autosense
!
vc-class ATM MyClass
 encapsulation aal5autoppp Virtual-Template1
!
interface ATM 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
!
! Configure PPPoE
!
vpdn enable
vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
!
ip cef
interface virtual-template 1
  ip unnumbered fastethernet 0/0/0
  ip route-cache cef
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
!
```

PPPoA PPPoE Autosense on Multiple VC Classes and Virtual Templates Example

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-mac** and **pppoe limit per-vc** commands are replaced by the **sessions per-mac limit** and **sessions per-vc limit** commands, respectively, in bba-group configuration mode. See the **sessions per-mac limit** and **sessions per-vc limit** commands for more information.

In the following example, PPPoA and PPPoE sessions are handled separately by two virtual templates.

```
ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
pppoe limit per-mac 1
pppoe limit per-vc 1
!
virtual-template 1 pre-clone 1500
virtual-template 2 pre-clone 1000
!
interface ATM0/0/0.3 multipoint
 no ip directed-broadcast
 class-int pppauto
!
interface ATM0/0/0.9 multipoint
 ip address 10.16.40.1 255.255.0.0
 no ip directed-broadcast
!
interface Virtual-Template1
 ip unnumbered ATM0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-1
 ppp authentication pap
!
interface Virtual-Template2
 ip unnumbered ATM0/0/0.9
 ip route-cache cef
 no ip directed-broadcast
 peer default ip address pool pool-2
 ppp authentication chap
!
interface fastethernet 0/0/0
 ip address 10.1.1.1 255.255.255.0
!
vc-class atm pppauto
 encapsulation aal5autoppp Virtual-Template2
!
```

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

Where to Go Next

If you want to identify a physical subscriber line for RADIUS communication with a RADIUS server, refer to the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.

Additional References

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

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Broadband access aggregation preparation tasks	Preparing for Broadband Access Aggregation

Standards

Standards	Title
Frame Relay Forum standard FRF.8	*Frame Relay to ATM Internetworking*

MIBs

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

RFCs

RFCs	Title
RFC 2364	*PPP over AAL5*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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

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

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

Table 2 Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Feature Name	Releases	Feature Configuration Information
PPP over ATM	12.1(1)	PPP over ATM enables a high-capacity central site router with an ATM interface to terminate multiple remote PPP connections. PPP over ATM provides security validation per user, IP address pooling, and service selection capability.
PPPoA/PPPoE Autosense for ATM PVCs	12.2(4)T 12.2(4)T3	The PPPoA/PPPoE autosense for ATM PVCs feature enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

Upstream PPPoX Connection Speed Transfer at LAC

The Upstream PPPoX Connection Speed Transfer at LAC feature allows the transfer of the upstream PPPoX session speed value at the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC). This transfer is accomplished by configuring the required speed on the ATM virtual circuit (VC) carrying the PPPoX session and then transferring this information into attribute-value (AV) pair 38 for transport from the LAC to the L2TP network server (LNS).

Note PPPoX is a term used to refer to PPPoE, PPPoA, and PPPoEoA. All are implementations of PPP over various delivery protocols such as Ethernet and ATM.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Upstream PPPoX Connection Speed Transfer at LAC

- You must understand the concepts described in the *Preparing for Broadband Access Aggregation* module.
- You must establish PPPoE sessions using the procedures in the *Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions* module.

Restrictions for Upstream PPPoX Connection Speed Transfer at LAC

The following restrictions apply to the Upstream PPPoX Connection Speed Transfer at LAC feature:

- For PPPoE, all sessions over the same VC must have the same send and receive speed.
- The upstream speed is informational and does not imply any policing or shaping of the session speed.

Information About Upstream PPPoX Connection Speed Transfer at LAC

Upstream PPPoX Connection Speed Transfer at LAC

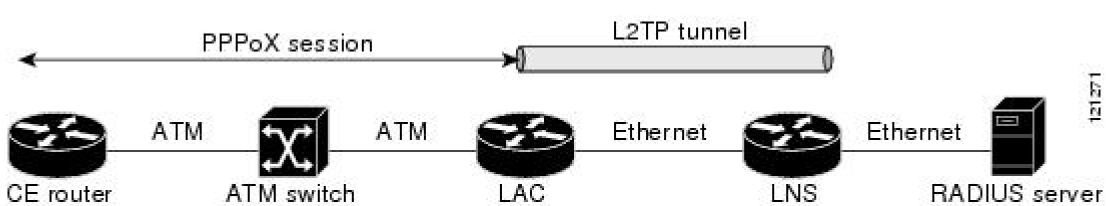
The send speed from the LAC to the remote destination is copied into AV pair 38 so that the session is symmetric at the LNS. The LNS does not do any policing of the upstream rate but verifies the session speed against the Service Level Agreement (SLA) before accepting it.

The transfer of the upstream PPPoX session speed at the LAC is done by:

- Configuring the required speed on the ATM virtual circuit carrying the PPPoX session.
- Transferring the information to AV pair 38 for transport from the LAC to the LNS.

The figure below shows how the Upstream PPPoX Connection Speed Transfer at LAC feature works.

Figure 8 Upstream PPPoX Connection Speed Transfer at LAC



Benefits of Upstream PPPoX Connection Speed Transfer at LAC

The Upstream PPPoX Connection Speed Transfer at LAC feature enables the configuration of an upstream PPPoX session speed, which is different from the downstream speed and allows the transfer of the upstream speed value from the LAC to the LNS. The default state (before this feature is enabled) is that the upstream speed and the downstream speed are the same. This feature implements changes that allows asymmetry in the upstream and downstream speeds.

This feature provides the following benefits:

- Allows support for asymmetric broadband service speeds such as asymmetric digital subscriber line (ADSL).
- Complies with RFC 2661 for L2TP.
- Is required for regulatory compliance in certain European countries; for example, Germany.

How to Configure Upstream Connection Speed Transfer at LAC

- Configuring Upstream PPPoX Connection Speed Transfer at the LAC, page 67

Configuring Upstream PPPoX Connection Speed Transfer at the LAC

The tasks in this section configure upstream PPPoX connection speed transfer at the LAC on a PVC or VC:

- Configuring Upstream PPPoX Connection Speed Transfer at LAC on a PVC, page 67
- Configuring Upstream PPPoX Connection Speed Transfer at LAC on VC, page 68

Configuring Upstream PPPoX Connection Speed Transfer at LAC on a PVC

Perform this task to configure the Upstream PPPoX Connection Speed Transfer feature at the LAC on a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port* **.** [*subinterface-number*{**mpls** | **multipoint**| **point-to-point**}]
4. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
5. **rx-speed** *incoming-cell-rate*
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *port* **.** [*subinterface-number*{**mpls** | **multipoint**| **point-to-point**}] **Example:** `Router(config)# interface atm 2/0.1 multipoint`	Enters subinterface configuration mode.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci* **Example:** `Router(config-subif)# range pvc 0/100 0/110`	Enters PVC-in-range configuration mode.
Step 5	**rx-speed** *incoming-cell-rate* **Example:** `Router(config-if-atm-range)# rx-speed 128`	Allows L2TP to send AV pair 38 with the given value to LNS. • The valid range for *incoming-cell-rate*for L2TP AVP is from 0 to 44209 kb/s.
Step 6	**exit** **Example:** `Router(config-if-atm-range)# exit`	Exits PVC-in-range configuration mode.

Configuring Upstream PPPoX Connection Speed Transfer at LAC on VC

Perform this task to configure the Upstream PPPoX Connection Speed Transfer at LAC on a VC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port* **.** [*subinterface-number*{**mpls** | **multipoint** | **point-to-point**}]
4. **pvc** [*name*] {*vpi/vci* | *vci*} [**ces** | **ilmi** | **qsaal** | **smds** | **l2transport**]
5. **rx-speed** *incoming-cell-rate*
6. **encapsulation** {**aal2** | **aal5auto** | **aal5autoppp virtual-template** *number* [**group** *group-name*] | **aal5ciscoppp virtual-template** *number* | **aal5mux** *protocol* | **aal5nlpid** | **aal5snap**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *port* **.** [*subinterface-number*{**mpls** | **multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 2/0.1 multipoint`	Enters subinterface configuration mode.
Step 4	**pvc** [*name*] {*vpi*/*vci* | *vci*} [**ces** | **ilmi** | **qsaal** | **smds** | **l2transport**] **Example:** `Router(config-subif)# pvc pvc1 0/100`	Enters PVC-class configuration mode.
Step 5	**rx-speed** *incoming-cell-rate* **Example:** `Router(config-if-atm-vc)# rx-speed 128`	Allows L2TP to send (AV) pair 38 with the given value to LNS.
Step 6	**encapsulation** {**aal2** | **aal5auto** | **aal5autoppp virtual-template** *number* [**group** *group-name*] | **aal5ciscoppp virtual-template** *number* | **aal5mux** *protocol* | **aal5nlpid** | **aal5snap**} **Example:** `Router(config-if-atm-vc)# encapsulation aal5snap`	Configures Logical Link Control (LLC) Subnetwork Access Protocol (SNAP) encapsulation on the PVC.
Step 7	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits PVC-class configuration mode.

Configuration Examples for Upstream PPPoX Connection Speed Transfer at LAC

Configuring Upstream PPPoX Connection Speed Transfer at LAC Example

The following examples show how to configure the upstream PPPoX connection speed transfer at LAC in PVC, range PVC, and PVC-in-range modes.

PVC Class

```
interface atm 6/0.110 multipoint
 pvc 0/600
 rx-speed 128
  encapsulation aal5snap
  exit
```

Range PVC

```
interface atm 6/0.110 multipoint
 range range-pppoa-1 pvc 100 4/199
  rx-speed 400
 exit
```

PVC-in-Range

```
interface atm 6/0.110 multipoint
  range range1 pvc 100 4/199
 pvc-in-range 0/300
 rx-speed 200
 shutdown
```

Additional References

The following sections provide references related to the upstream PPPoX connection speed transfer.

Related Documents

Related Topic	Document Title
Configuring VC classes	"Configuring VC Classes" section in the "Configuring ATM" module in the*Cisco IOS Wide-Area Networking Configuration Guide* .
Understanding the Unspecified Bit Rate+ (UBR+) service category for ATM VCs	"Understanding the UBR+ Service Category for ATM VCs" module in ATM (Asynchronous Transfer Mode) Technical Support

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation module
Preparing for broadband access aggregation task	Preparing for Broadband Access Aggregation module
BBDSL commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Cisco IOS commands	Cisco IOS Master Commands 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 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 2 Tunneling Protocol "L2TP"*

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 Upstream PPPoX Connection Speed Transfer at LAC

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 Upstream PPPoX Connection Speed Transfer at LAC

Feature Name	Releases	Feature Information
Upstream PPPoX Connection Speed Transfer at LAC	12.2(15)B 12.2(4)T 12.2(33)SRE	The Upstream PPPoX Connection Speed Transfer at LAC feature allows the transfer of the upstream PPPoX session speed value at the LAC. The following command was introduced:**rx-speed**.

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Providing Session Limit Support

The PPP over Ethernet Session Limit feature enables you 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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Providing Session Limit Support

Benefits of Providing Session Limit Support

The PPPoE Session Limit 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 sub-interfaces as well as ATM interfaces and sub-interfaces.

How to Provide Session Limit Support

Specifying the Maximum Number of PPPoE Sessions on the 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 BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode. • *name* --Identifies the broadband aggregation (BBA) group. You can have multiple BBA groups. • **global** --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 which virtual template will be used to clone virtual access interfaces for all PPPoE ports that use this PPPoE profile.

	Command or Action	Purpose
Step 5	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac limit 1000`	(Optional) Sets the maximum number of PPPoE sessions allowed per MAC session limit in a PPPoE profile. The default 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 sub-interface. The default is 100. **Note** The per-VLAN limit is only applicable to Gigabit Ethernet subinterfaces (802.1q VLANs).
Step 7	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit 2000`	(Optional) Sets the maximum number of PPPoE sessions allowed per VC session limit in a PPPoE profile. The default is 100. **Note** The per-vc limit is applicable only to ATM interfaces and sub-interfaces.
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 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. The default value is 100.

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

Configuration Examples for Providing Session Limit Support

- Specifying the Maximum Number of PPPoE Sessions on a Router Example, page 79
- Specifying the Maximum Number of PPPoE Sessions on a Gigabit Ethernet Interface Example, page 79

Specifying the Maximum Number of PPPoE Sessions on a Router Example

The following example shows a limit of 32,000 PPPoE sessions configured 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
```

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

The following example shows a limit of ten PPPoE sessions on the Gigabit Ethernet interface:

```
interface GigabitEthernet1/0/0
  pppoe enable
  pppoe max-sessions 10
```

The following example shows a limit of ten PPPoE sessions on the Gigabit Ethernet subinterface using the **encapsulation**command:

```
interface GigabitEthernet0/0/0.1
  encapsulation dot1q 2
  pppoe enable
  pppoe max-sessions 10
```

Additional References

The following sections provide references related to supporting session limits.

Related Documents

Related Topic	Document Title
Broadband access aggregation of PPPoE sessions	Understanding Broadband Access Aggregation
Task for preparing for broadband access aggregation	Preparing for broadband access aggregation
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Additional information about commands used in this document	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 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 Providing 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 4 Feature Information for Providing Session Limit Support

Feature Name	Releases	Feature Information
PPP over Ethernet (PPPoE) Session Limit	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(4)T 15.0(1)M 12.2(33)SRE	The PPP over Ethernet (PPPoE) Session Limit 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. The following commands were introduced or modified: **sessions per-mac limit, sessions per-vlan limit, sessions per-vc limit, sessions max limit, pppoe max-sessions**

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.

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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Monitoring PPPoE Sessions with SNMP

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

Restrictions for Monitoring PPPoE Sessions with SNMP

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

Information About Monitoring PPPoE Sessions with SNMP

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

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit max-sessions**command is replaced by the **sessions max limit**command in BBA group configuration mode. See the **sessions max limit**command for more information.

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 **pppoe limit max-sessions** and **pppoe max-sessions** commands.

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://www.cisco.com/go/mibs .

Table 5 PPPoE Session Count MIB Objects and Tables

Object or Table	Description
cPppoeSystemCurrSessions	Number of PPPoE sessions active on the router.
cPppoeSystemHighWaterSessions	Total number of PPPoE sessions configured on the router since the system was initialized.

Object or Table	Description
cPppoeSystemMaxAllowedSessions	Number of PPPoE sessions that can be configured on the router.
cPppoeSystemThresholdSessions	Threshold value of PPPoE sessions that can be configured on the router.
cPppoeSystemExceededSessionErrors	Accumulated number of errors on the router that have occurred because the cPppoeSystemCurrSessions value exceeded the cPppoeSystemMaxAllowedSessions value.
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 SNMP Monitoring of PPPoE Sessions

Enabling PPPoE Session Count SNMP Traps

Perform this task to enable SNMP traps that send notification messages when PPPoE session thresholds have been reached.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pppoe**
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	**snmp-server enable traps pppoe** **Example:** `Router(config)# snmp-server enable traps pppoe`	Enables PPPoE session count SNMP notifications.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring the PPPoE Session-Count Threshold for the Router Using VPDN Groups

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit max-sessions**command is replaced by the **sessions max limit**command in BBA group configuration mode. See the **sessions max limit** command for more information.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **accept-dialin**
5. protocol pppoe
6. **virtual-template** *template-number*
7. **pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
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	**vpdn-group** *name* **Example:** `Router(config)# vpdn group dialingroup1`	Associates a virtual private dialup network (VPDN) group with a customer or VPDN profile and enters VPDN group configuration mode.

	Command or Action	Purpose
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept dialin`	Creates an accept dialin VPDN group and enters VPDN dialin access configuration mode.
Step 5	protocol pppoe **Example:** `Router(config-vpdn-acc-in)# protocol pppoe`	Configures the Layer 2 Tunneling Protocol (L2TP) that the VPDN subgroup will use.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-vpdn-acc-in)# virtual template 100`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 7	**pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-vpdn-acc-in)# pppoe limit max-sessions 4000 threshold-sessions 3000`	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 8	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Exits VPDN dialin access configuration mode and returns to VPDN group configuration mode.

Configuring the PPPoE Session-Count Threshold for the Router Using BBA Groups

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe global**
4. **virtual-template** *template-number*
5. **sessions max limit** *number-of-sessions* [**threshold** *number-of-sessions*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe 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 100`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 5	**sessions max limit** *number-of-sessions* [**threshold** *number-of-sessions*] **Example:** `Router(config-bba-group)# sessions max limit 4000 threshold 3000`	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
Step 6	**exit** **Example:** `Router(config-bba-group)# exit`	Exits BBA group configuration mode and returns to global configuration mode.

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. **interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters interface configuration mode. **Note** To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 5/120`	Configures the 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.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits ATM virtual circuit configuration mode and returns to interface configuration mode.

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. **vc-class atm** *name*
4. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
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	**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 ATM VC class configuration mode.

	Command or Action	Purpose
Step 4	**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 5	**exit** **Example:** `Router(config-vc-class)# exit`	Exits ATM VC class configuration mode and returns to global configuration mode.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **range** [range-name] **pvc** start-vpi/start-vci end-vpi/end-vci
5. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 0/0/0.3 point-to-point`	Configures the ATM interface and enters interface configuration mode. **Note** To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.
Step 4	**range** [range-name] **pvc** start-vpi/start-vci end-vpi/end-vci **Example:** `Router(config-if)# range pvc 3/100 3/105`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 5	**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 6	**exit** **Example:** `Router(config-if-atm-range)# exit`	Exits ATM PVC range configuration mode and returns to global configuration mode.

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. **interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* /end-vci
5. **pvc-in-range** [*pvc-name*] [*vpi* / *vci*]
6. **pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* [**.** *subinterface-number* {**mpls** | **multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm6/0.110 multipoint`	Configures the ATM interface and enters interface configuration mode. **Note** To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.
Step 4	**range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / end-vci **Example:** `Router(config-if)# range range1 pvc 3/100 4/199`	Defines a range of ATM PVCs and enters ATM PVC range configuration mode.
Step 5	**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 6	**pppoe max-sessions** *number-of-sessions* [**threshold-sessions** *number-of-sessions*] **Example:** `Router(config-if-atm-range-pvc)# pppoe max-sessions 10 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.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if-atm-range-pvc)# exit`	Exits ATM PVC in-range configuration mode and returns to ATM PVC range configuration mode.

Verifying PPPoE Session-Count Thresholds

Use the following task to verify PPPoE session-count thresholds:

SUMMARY STEPS

1. **enable**
2. **more system:running config**

DETAILED STEPS

Step 1 **enable**

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

Example:

```
Router> enable
```

Step 2 **more system:running config**

Use this command to display the running configuration.

Example:

```
Router# more system:running config
Building configuration...
Current configuration:
!
version 12.3
no service udp-small-servers
no service tcp-small-servers
!
hostname Router2
!
.
.
.
!
end
```

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 interface atm** *interface-number*
4. **debug pppoe events interface atm** *interface-number* **vc** *vci-value*
5. **show vpdn** [**session**] [**packets**] [**tunnel**] [**all**]

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 172.16.63.17 on Ethernet0
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 172.16.63.17
```

Step 3 **debug pppoe errors interface atm** *interface-number*

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 interface atm** *interface-number* **vc** *vci-value*

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**] [**packets**] [**tunnel**] [**all**]

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
```

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 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

PPPoE Session-Count Threshold for the Router Example

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit max-sessions**command is replaced by the **sessions max limit**command in BBA group configuration mode. See the **sessions max limit** command for more information.

The following example shows a limit of 4000 PPPoE sessions configured for the router through VPDN groups. 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.

```
vpdn enable
no vpdn logging
!
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
pppoe limit max-sessions 4000 threshold-sessions 3000
```

The following example shows a limit of 4000 PPPoE sessions configured for the router through BBA groups. 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 global
 virtual-template 1
  sessions max limit 4000 threshold 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
 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
  protocol pppoe
```

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

The following example shows a limit of ten PPPoE sessions configured for pvc1. The PPPoE session-count threshold is set at three sessions, so when the number of PPPoE sessions for the PVC reaches three, an SNMP trap will be generated.

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 3/104
   pppoe max-sessions 10 threshold-sessions 3
```

Where to Go Next

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

Additional References

The following sections provide references related to monitoring PPPoE sessions with SNMP.

Related Documents

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

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
PPPoE Session Count MIB	To locate and download MIBs for selected platforms, Cisco IOS 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/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 6 Feature Information for Monitoring PPPoE Sessions with SNMP

Feature Name	Releases	Feature Configuration Information
PPPoE Session Count MIB	12.2(1)DC 12.2(8)T 12.2(33)SRC	This feature provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPP over Ethernet sessions configured on permanent virtual circuits (PVCs) and on a router. The following commands were introduced or modified: **pppoe limit max-sessions**, **pppoe max-sessions**, **sessions max limit**.

Glossary

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

MIB --Management Information Base. 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 (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

PVC --Permanent Virtual Circuit. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, PVC also stands for permanent virtual connection.

SNMP --Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents and is exclusively used in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

trap --A message from an SNMP agent alerting the SNMP manager to a condition on the network.

VCI --Virtual Channel Identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transit on its way to its final destination.

VCL --Virtual Channel Link. Connection between two ATM devices.

PPP over Ethernet Client

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers.

PPPoE is a commonly used application in the deployment of digital subscriber lines (DSLs). The PPP over Ethernet Client feature expands PPPoE functionality by providing support for PPPoE on the client and the server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for PPP over Ethernet Client

PPP connections must be established between two endpoints over a serial link.

Restrictions for PPPoE Client

- For PPPoE over ATM, one permanent virtual circuit (PVC) supports multiple PPPoE clients, allowing multiple PPPoE sessions to run concurrently on the same PVC. An ATM PVC is allowed to be a member of several dialer pools as long as the dialer pool number is unique.
- For PPPoE, each PPPoE client must use a separate dialer interface and a separate dialer pool.

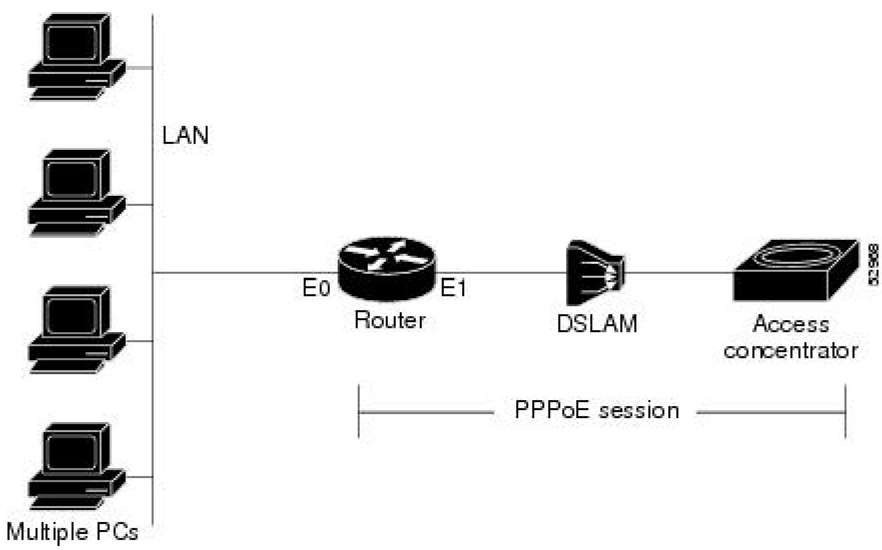
- For the PPPoE--Max-Payload Support on Client feature the physical interface should support a maximum transmission unit (MTU) greater than 1500.
- For the PPPoE--Max-Payload Support on Client feature, appropriate configuration is required on the Broadband Remote Access Server (BRAS). For more information, see the "PPP-Max-Payload and IWF PPPoE Tag Support" module.

Information About PPP over Ethernet Client

PPPoE Client Network Topology

The PPP over Ethernet Client feature provides PPPoE client support on routers on customer premises. Before the introduction of this feature, Cisco IOS software supported PPPoE on the access server side only. The figure below shows the typical network topology for configuring a PPPoE client on an Ethernet interface (E1 interface).

Figure 9 Typical Network Topology for PPPoE Deployment



PPPoE Client Support on ATM PVCs and Ethernet Interfaces

The PPPoE Client feature provides PPPoE client support on ATM PVCs and Ethernet interfaces. A dialer interface must be used for cloning virtual access.

Prior to Cisco IOS Release 12.4(15)T, one ATM PVC supported one PPPoE client. With the introduction of the Multiple PPPoE Client feature in Cisco IOS Release 12.4(15)T, one ATM PVC supports multiple PPPoE clients, allowing second line connection and redundancy. Multiple PPPoE clients can run concurrently on different PVCs, but each PPPoE client must use a separate dialer interface and a separate dialer pool.

Multiple PPPoE client sessions can be configured on an Ethernet interface, but each session must use a separate dialer interface and a separate dialer pool.

• PPPoE--Max-Payload Support on Client, page 107

PPPoE--Max-Payload Support on Client

PPPoE, as described in RFC 2516, mandates a maximum negotiated Maximum Receive Unit (MRU) of 1492. This means that a PPPoE data packet cannot accommodate more than 1492 bytes of payload. To overcome this limitation, the client can use the PPP-Max-Payload tag (defined in RFC 4638) and negotiate a higher MRU with the Broadband Remote Access Server (BRAS). Use the **pppoe-client ppp-max-payload** command to send the PPP Max-Payload tag in PPPoE control packets to negotiate a higher MRU. A PPP Max-Payload tag allows a PPPoE client to override the MRU of 1492 by providing a maximum size for the PPP payload in both the sending and receiving directions.

The PPPoE client sends the PPPoE Max-Payload tag in a PPPoE Active Discovery Initiation (PADI) packet and if the PPPoE server can support a Maximum Transmission Unit (MTU)/Maximum Receive Unit (MRU) higher than 1492 octets, it responds with an echo of the clients tag in the PPPoE Active Discovery Offer (PADO) packet. The client sends the same tag in the PPPoE Active Discovery Request (PADR), and the server echoes the client tag in a PPPoE Active Discovery Session-confirmation (PADS) packet.

The **pppoe-client ppp-max-payload** command can only be configured when the PPPoE client dialer configuration is done. When the **pppoe-client ppp-max-payload** command is configured without the dialer configuration, an error message is displayed. If the dialer configuration is removed, the PPP max-payload configuration is also removed.

PPP over Ethernet Client Session Initiation

A PPPoE session is initiated by the PPPoE client. If the session has a timeout or is disconnected, the PPPoE client will immediately attempt to reestablish the session.

The following steps describe the exchange of packets that occurs when a PPPoE client initiates a PPPoE session:

1. The client broadcasts a PPPoE active discovery initiation (PADI) packet.
2. When the access concentrator receives a PADI packet that it can serve, it replies by sending a PPPoE active discovery offer (PADO) packet to the client.
3. Because the PADI packet was broadcast, the host may receive more than one PADO packet. The host looks through the PADO packets it receives and chooses one. The choice can be based on the access concentrator name or on the services offered. The host then sends a single PPPoE active discovery request (PADR) packet to the access concentrator that it has chosen.
4. The access concentrator responds to the PADR packet by sending a PPPoE active discovery session-confirmation (PADS) packet. At this point, a virtual access interface is created that will then negotiate PPP and the PPPoE session will run on this virtual access.

If a client does not receive a PADO packet for a PADI packet already received, the client sends out a PADI packet at predetermined intervals. That interval length is doubled for every successive PADI packet that does not evoke a response, until the interval reaches the configured maximum.

If PPP negotiation fails or the PPP line protocol is brought down for any reason, the PPPoE session and the virtual access will be brought down and the client will wait for a predetermined number of seconds before trying to establish another PPPoE session.

How to Configure a PPPoE Client

Configuring a PPPoE Client in Releases Prior to Cisco IOS Release 12.2(13)T

Perform the following tasks to configure a PPPoE client in releases prior to Cisco IOS release 12.2(13)T:

Enabling PPPoE in a VPDN Group

Perform this task to enable PPPoE in a virtual private dial-up network (VPDN) group.

Note

This task applies only to releases prior to Cisco IOS Release 12.2(13)T.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. **vpdn-group** *name*
5. **request-dialin**
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	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables virtual private dialup networking.
Step 4	**vpdn-group** *name* **Example:** `Router(config)# vpdn-group group1`	Associates a VPDN group with a customer or a VPDN profile and enters VPDN group configuration mode.
Step 5	**request-dialin** **Example:** `Router(config-vpdn)# request-dialin`	Creates a request-dialin VPDN subgroup and enters the VPDN request dialin configuration mode.
Step 6	**protocol pppoe** **Example:** `Router(config-vpdn-req-in)# protocol pppoe`	Enables the VPDN subgroup to establish PPPoE sessions.
Step 7	**end** **Example:** `Router(config-vpdn-req-in)# end`	Exits VPDN request dialin configuration mode and returns to privileged EXEC mode.

Configuring a PPPoE Client on an ATM PVC

Perform this task to configure a PPPoE client on an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe-client dial-pool-number** *number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Configures an ATM interface.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 1/100`	Creates an ATM PVC and enters ATM virtual circuit configuration.
Step 5	**pppoe-client dial-pool-number** *number* **Example:** `Router(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures the PPPoE client and specifies the dialer interface to use for cloning on the PVC.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Returns to privileged EXEC mode.

Note If you make any changes to the PVC configuration after the PPPoE client session is established, the session is automatically terminated and reestablished.

Configuring a PPPoE Client on an Ethernet Interface

Perform this task to configure a PPPoE client on an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *number*
4. **pppoe-client dial-pool-number** *number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *number* **Example:** `Router(config)# interface ethernet 0`	Configures an Ethernet interface and enters interface configuration mode.

	Command or Action	Purpose

Step 4	**pppoe-client dial-pool-number** *number*
	
	Example:
	
	`Router(config-if)#`
	` pppoe-client dial-pool-number 1`
		Configures the PPPoE client and specifies the dialer interface to use for cloning.

Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring the Dialer Interface

Perform this task to configure the dialer interface to be used for cloning on the PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dialer** *number*
4. **mtu** *bytes*
5. **encapsulation ppp**
6. **ip address negotiated**
7. **dialer pool** *number*
8. **dialer-group** *group-number*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface dialer** *number* **Example:** `Router(config)# interface dialer 1`	Configures a dialer interface.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1492`	Adjusts the maximum packet size or maximum transmission unit (MTU) size. The range is from 64 to 17940. **Note** Cisco recommends that you set the MTU to 1492 bytes. This value accommodates a PPPoE header encapsulation of 8 bytes in the Ethernet frame payload.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation type of the interface to Point-to-Point Protocol.
Step 6	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for the interface be obtained via PPP/IP Control Protocol (PPP/IPCP) address negotiation.

Step 7	**dialer pool** *number*
	
	Example:
	
	`Router(config-if)#`
	` dialer pool 1`
		Specifies the dialing pool to use to connect to a specific destination subnetwork.

Step 8	**dialer-group** *group-number*
	
	Example:
	
	`Router(config-if)#`
	` dialer-group 1`
		Configures an interface to belong to a specific dialing group.

Step 9	**end** **Example:** `Router(config-if)# end`	Exits interface configuration and returns to privileged EXEC mode.

Clearing PPPoE Client Sessions

Perform this task to clear PPPoE client sessions.

Note This task applies only to releases prior to Cisco IOS Release 12.2(13)T.

>

SUMMARY STEPS

1. **enable**
2. **clear vpdn tunnel pppoe**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear vpdn tunnel pppoe** **Example:** `Router# clear vpdn tunnel pppoe`	Terminates the PPPoE client session and causes the PPPoE client to try to reestablish the session immediately.

Note To terminate a PPPoE client session, use the **no pppoe-client dial-pool-number** command in interface configuration mode or interface-ATM-VC configuration mode.

Verifying the PPPoE Client

Perform this task to verify PPPoE client configuration.

This task assumes that the PPPoE client has been configured.

SUMMARY STEPS

1. **enable**
2. **show vpdn**
3. **show vpdn session packet**
4. **show vpdn session all**
5. **show vpdn tunnel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vpdn** **Example:** `Router# show vpdn`	Displays information about the active Layer 2 Forwarding (L2F) protocol tunnel and L2F message identifiers in a VPDN.
Step 3	**show vpdn session packet** **Example:** `Router# show vpdn session packet`	Displays PPPoE session statistics.
Step 4	**show vpdn session all** **Example:** `Router# show vpdn session all`	Displays PPPoE session information for each session ID.
Step 5	**show vpdn tunnel** **Example:** `Router# show vpdn tunnel`	Displays PPPoE session count for the tunnel.

Troubleshooting PPPoE Client Sessions

Perform this task to troubleshoot the PPPoE client.

Note This task applies only to releases prior to Cisco IOS Release 12.2(13)T.

SUMMARY STEPS

1. **enable**
2. **debug vpdn pppoe-data**
3. **debug vpdn pppoe-errors**
4. **debug vpdn pppoe-events**
5. **debug vpdn pppoe-packets**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug vpdn pppoe-data** **Example:** `Router# debug vpdn pppoe-data`	Displays PPPoE session data packets.
Step 3	**debug vpdn pppoe-errors** **Example:** `Router# debug vpdn pppoe-errors`	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be terminated.
Step 4	**debug vpdn pppoe-events** **Example:** `Router# debug vpdn pppoe-events`	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
Step 5	**debug vpdn pppoe-packets** **Example:** `Router# debug vpdn pppoe-packets`	Displays each PPPoE protocol packet exchanged.

Configuring a PPPoE Client in Cisco IOS Release 12.2(13)T 12.4T and Later Releases

• Configuring a PPPoE Client on an ATM PVC, page 117

Configuring a PPPoE Client on an ATM PVC

Perform this task to configure a PPPoE client on an ATM PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number*
4. **pvc** [*name*] *vpi* / *vci*
5. **pppoe-client dial-pool-number** *number*
6. **pppoe-client ppp-max-payload** *max-value*
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	**interface atm** *number* **Example:** `Router(config)# interface atm 0`	Configures an ATM interface.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-if)# pvc 1/100`	Creates an ATM PVC and enters ATM virtual circuit configuration.

	Command or Action	Purpose
Step 5	**pppoe-client dial-pool-number** *number* **Example:** `Router(config-if-atm-vc)# pppoe-client dial-pool-number 1`	Configures the PPPoE client and specifies the dialer interface to use for cloning on the PVC. **Note** If Cisco IOS Release 12.4(15)T or a later release is running, you can configure multiple PPPoE clients on the same PVC. For earlier releases, one PVC supports only one PPPoE client.

Step 6	**pppoe-client ppp-max-payload** *max-value*
	
	Example:
	
	`Router(config-if-atm-vc)#`
	
	`pppoe-client ppp-max-payload 1500`
		Configures the PPPoE client to send a PPP Max-Payload tag in PPPoE control packets.

Step 7	**end**
	
	Example:
	
	`Router(config-if-atm-vc)#`
	
	`end`
		Exits ATM virtual circuit configuration mode and returns to privileged EXEC mode.

Note If you make any changes to the PVC configuration after the PPPoE client session is established, the session is automatically terminated and reestablished.

Configuring a PPPoE Client on an Ethernet Interface

Perform this task to configure a PPPoE client on an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *number*
4. **pppoe-client dial-pool-number** *number*
5. **pppoe-client ppp-max-payload** *max-value*
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 ethernet** *number* **Example:** `Router(config)# interface ethernet 0`	Configures an Ethernet interface.

Step 4	**pppoe-client dial-pool-number** *number*
	
	Example:
	
	`Router(config-if)#`
	`pppoe-client dial-pool-number 1`
		Configures the PPPoE client and specifies the dialer interface to use for cloning. You can configure multiple PPPoE clients on the same PVC.

Step 5	**pppoe-client ppp-max-payload** *max-value*
	
	Example:
	
	`Router(config-if)#`
	
	`pppoe-client ppp-max-payload 1500`
		Configures the PPPoE client to send a PPP Max-Payload tag in PPPoE control packets.

Step 6	**end**
	
	Example:
	
	`Router(config-if)#`
	
	`end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a PPPoE Client on an Ethernet Subinterface

Perform this task to configure a PPPoE client on an Ethernet subinterface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *number*
4. **encap dot1Q** *vlan-id* [**native**]
5. **pppoe-client dial-pool-number** *number*
6. **pppoe-client ppp-max-payload** *max-value*
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	**interface ethernet** *number* **Example:** `Router(config)# interface ethernet 0/0.10`	Configures an Ethernet subinterface, and enters Ethernet subinterface mode.
Step 4	**encap dot1Q** *vlan-id* [**native**] **Example:** `Router(config-subif)# encap dot1Q 10`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface.

Step 5	**pppoe-client dial-pool-number** *number*
	
	Example:
	
	`Router(config-subif)#`
	` pppoe-client dial-pool-number 1`
		Configures the PPPoE client and specifies the dialer interface to use for cloning.

	Command or Action	Purpose

Step 6	**pppoe-client ppp-max-payload** *max-value*
	
	Example:
	
	`Router(config-subif)#`
	
	`pppoe-client ppp-max-payload 1500`
		Configures the PPPoE client to send a PPP Max-Payload tag in PPPoE control packets.

Step 7	**end**
	
	Example:
	
	`Router(config-subif)#`
	
	`end`
		Exits subinterface configuration mode and returns to privileged EXEC mode.

Configuring the Dialer Interface

Perform this task to configure the dialer interface to be used for cloning on the PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface dialer** *number*
4. **mtu** *bytes*
5. **encapsulation ppp**
6. **ip address negotiated**
7. **dialer pool** *number*
8. **dialer-group** *group-number*
9. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dialer** *number* **Example:** `Router(config)# interface dialer 1`	Configures a dialer interface.
Step 4	**mtu** *bytes* **Example:** `Router(config-if)# mtu 1492`	Adjusts the maximum packet size or MTU size. **Note** Cisco recommends that you set the MTU to 1492 bytes. This value accommodates a PPPoE header encapsulation of 8 bytes in the Ethernet frame payload.
Step 5	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation type of the interface to the Point-to-Point protocol.
Step 6	**ip address negotiated** **Example:** `Router(config-if)# ip address negotiated`	Specifies that the IP address for the interface is obtained via PPP/IPCP address negotiation.

Step 7	**dialer pool** *number*
	
	Example:
	
	`Router(config-if)#`
	`dialer pool 1`
		Specifies the dialing pool to use to connect to a specific destination subnetwork.

Step 8	**dialer-group** *group-number*
	
	Example:
	
	`Router(config-if)#`
	`dialer-group 1`
		Configures an interface to belong to a specific dialing group.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Clearing PPPoE Client Sessions

Perform this task to clear PPPoE client sessions.

Note This task applies only to Cisco IOS Release 12.2(13)T and later releases.

>

SUMMARY STEPS

1. **enable**
2. **clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] | **rmac** *mac-address* | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] | **rmac** *mac-address* | **all**} **Example:** `Router# clear pppoe all`	Clears the PPPoE client session and causes the PPPoE client to try immediately to reestablish the session.

Note To permanently terminate a PPPoE client session, use the **no pppoe-client dial-pool-number**command in interface configuration mode or interface-ATM-VC configuration mode.

Verifying the PPPoE Client

Perform this task to verify PPPoE client configuration.

Note This task applies only to Cisco IOS Release 12.2(13)T and later releases.

>

SUMMARY STEPS

1. **enable**
2. **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	**show pppoe session** [**all** | **packets**] **Example:** `Router# show pppoe session`	Displays information about currently active PPPoE sessions.

Troubleshooting PPPoE Client Sessions

Perform this task to troubleshoot the PPPoE client.

Note This task applies only to Cisco IOS Release 12.2(13)T and later releases.

>

SUMMARY STEPS

1. **enable**
2. **debug pppoe** {**data** | **errors** | **events** | **packets**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug pppoe** {**data** | **errors** | **events** | **packets**} **Example:** `Router# debug pppoe errors`	Displays debugging information for PPPoE sessions.

Configuration Examples for PPPoE Client

Examples PPPoE Client in Releases Prior to Cisco IOS Release 12.2(13)T

In the following example, a PPPoE client is configured on a PVC on the ATM interface 0. The PPPoE client uses the dialer interface 1 as its virtual access interface.

```
vpdn enable
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface atm0
 pvc 1/100
  pppoe-client dial-pool-number 1
!
interface dialer 1
 ip address negotiated
 dialer pool 1
 dialer-group 1
!
```

In the following example, two PPPoE client sessions are configured on an Ethernet interface. Each PPPoE client uses a separate dialer interface and a separate dialer pool.

```
vpdn enable
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface ethernet1/1
 pppoe-client dial-pool-number 1
 pppoe-client dial-pool-number 2
!
interface dialer 1
 ip address negotiated
```

```
 dialer pool 1
 dialer-group 1
!
interface dialer 2
 ip address negotiated
 dialer pool 2
 dialer-group 2
```

Examples PPPoE Client in Cisco IOS Release 12.2(13)T and Later Releases

The following example shows how to configure a PPPoE client on an Ethernet interface. Note that in Releases 12.2(13)T and later it is not necessary to configure a global VPDN group before configuring the PPPoE client.

```
interface Ethernet 0
 pppoe-client dial-pool-number 1
 pppoe-client ppp-max-payload 1500
interface Dialer 1
 ip address negotiated
 dialer pool 1
 mtu 1492
```

The following example shows how to configure multiple PPPoE clients on an ATM VC. Note that in Releases 12.4(15)T or a later release, more than one PPPoE session is supported on a single PVC.

```
interface ATM0
 no ip address
 no ip mroute-cache
 no atm ilmi-keepalive
 pvc 4/20
  pppoe-client dial-pool-number 1
  pppoe-client dial-pool-number 2
  pppoe-client ppp-max-payload 1500
 !
end
```

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*
VPDN features	*Cisco IOS VPDN Configuration Guide*
VPDN and PPPoE commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
PPP over Frame Relay	*Cisco IOS Wide-Area Networking Configuration Guide*

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 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)*
RFC 4638	*Accommodating a Maximum Transit Unit/ Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol 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 PPP over Ethernet Client

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

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

Table 7 Feature Information for PPP over Ethernet Client

Feature Name	Releases	Feature Information
PPPoE--Max-Payload Support on Client	15.1(4)M	This feature supports the PPPoE client to send a PPP Max-Payload tag in PPPoE control packets. This feature is based on RFC 4638. The following command was introduced or modified: **pppoe-client ppp-max-payload**.
PPP over Ethernet Client	12.2(2)T 12.2(13)T 12.4(15)T 15.0(1)M	This feature was introduced. In Cisco IOS Release 12.2(13)T, PPPoE client functionality was separated from VPDN functionality, resulting in changes to PPPoE client configuration. In the Cisco IOS Release 12.4(15)T, support was added for multiple PPPoE sessions per VC. No new commands were introduced or modified.
PPP over Ethernet Subinterface	12.4(20)T	Support was added for PPPoE clients on Ethernet subinterfaces.

PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature provides two enhancements to PPP over Ethernet (PPPoE) over IEEE 802.1Q VLAN functionality:

- It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.
- It adds ATM permanent virtual circuit (PVC) support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

PPPoE over IEEE 802.1Q VLAN support can be configured without using subinterfaces on the PPPoE server only.

ATM PVC support for PPPoE over IEEE 802.1Q VLANs can be configured only on the PPPoE server.

It is not possible to shut down traffic for individual VLANs that are configured on the main interface. Individual VLANs that are configured on subinterfaces can be shut down.

A VLAN range can be configured on a main interface at the same time that VLANs outside the range are configured on subinterfaces of the same main interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time.

Information About PPPoE over VLAN Configuration Limit Removal and ATM Support

To configure PPPoE over IEEE 802.1Q VLAN support on an interface rather than a subinterface, and to configure ATM support for PPPoE over IEEE 802.1Q VLANs, you should understand the following concepts:

PPPoE over VLAN Configuration Without Using Subinterfaces

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature removes the requirement for each PPPoE VLAN to be created on a subinterface. Allowing more than one PPPoE VLAN to be configured on a main interface increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

Individual VLANs or a range of VLANs can be configured on an interface. You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface.

PPPoE over VLAN Support on ATM PVCs

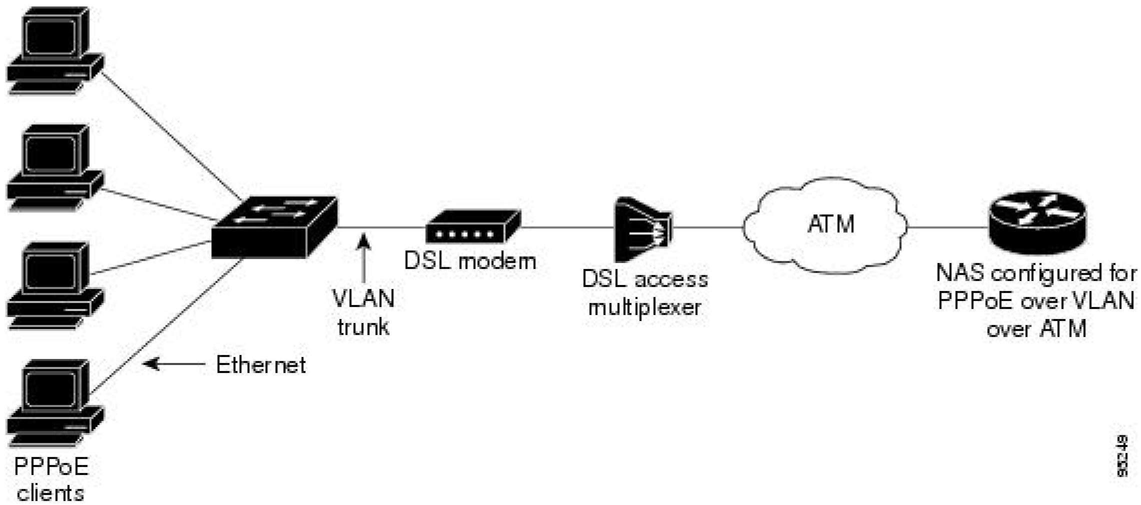
The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature enables ATM PVCs to process PPPoE over VLAN packets that use bridged RFC 1483 encapsulation. This capability allows PPPoE traffic from different IEEE 802.1Q VLANs to be multiplexed over the same ATM PVC.

The figure below shows a sample network topology that implements PPPoE over VLAN on ATM PVCs. In this topology, a service provider is using an Ethernet switch to provide Ethernet service to home users and a single PVC to provide the switch with WAN access. The home users use PPPoE to access services on the network access server (NAS). Each port on the switch is assigned a separate VLAN, and the VLANs are trunked over a Fast Ethernet or Gigabit Ethernet interface that is connected to a digital subscriber line (DSL) modem acting as a bridge.

The IEEE 802.1Q VLAN-encapsulated traffic coming in from the Ethernet switch trunk is encapsulated in RFC 1483 bridged encapsulation by the DSL modem and sent across the ATM WAN to the NAS. The NAS, which is configured to support PPPoE over VLANs over ATM PVCs, will extract the PPPoE packet from the PPPoE over IEEE 802.1Q VLAN over RFC 1483 bridged encapsulation and provide PPPoE services to the user.

In the downlink, the NAS sends packets in PPPoE over IEEE 802.1Q VLAN over RFC 1483 bridged encapsulation. The DSL modem strips off the RFC 1483 encapsulation and forwards the IEEE 802.1Q VLAN packets across the trunk to the switch. The switch then sends the Ethernet packets to the port associated with the IEEE 802.1 VLAN ID.

Figure 10 Sample Network Topology for PPPoE over IEEE 802.1Q VLANs over ATM



Benefits of PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature has the following benefits:

- Increases the number of VLANs that can be configured on a router to 4000 VLANs per interface by removing the requirement for each PPPoE VLAN to be configured on a subinterface.
- Provides support for PPPoE over VLANs over ATM interfaces using RFC 1483 bridged encapsulation

How to Configure PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

Configuring PPPoE over IEEE 802.1Q VLAN Support on an Ethernet Interface

Perform this task to configure PPPoE over IEEE 802.1Q VLAN support on an Ethernet interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **vlan-id dot1q** *vlan-id*
   -
   - **vlan-range dot1q** *start-vlan-id end-vlan-id*
5. **pppoe enable** [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/2`	Specifies the interface to be configured and enters interface configuration mode.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **vlan-id dot1q** *vlan-id*
	•
	• **vlan-range dot1q** *start-vlan-id end-vlan-id*
	
	Example:
	`Router(config-if)# vlan-id dot1q 0`
	
	Example:
	
	Example:
	`Router(config-if)# vlan-range dot1q 0 60`
		Enables IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface.
		or
		Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface.

Step 5	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-if-vlan-range)# pppoe enable group pppoe1`	Enables PPPoE sessions over a specific VLAN or a range of VLANs.

Configuring an ATM PVC to Support PPPoE over IEEE 802.1Q VLAN Traffic

Perform this task to configure an ATM PVC to support RFC 1483 bridge encapsulated PPPoE over IEEE 802.1Q VLAN traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* **.** *subinterface-number* {**multipoint | point-to-point}**
4. **pvc** [*name*] *vpi* / *vci*
5. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* **.** *subinterface-number* {**multipoint** | **point-to-point**} **Example:** `Router(config)# interface atm 2/0.1 multipoint`	Configures an ATM multipoint subinterface and enters subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc 0/60`	Configures a PVC and enters ATM VC configuration mode.
Step 5	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-if-atm-vc)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs on an ATM PVC.

Configuring a VC Class for PPPoE over IEEE 802.1Q VLAN Support

Perform this task to configure support for PPPoE over IEEE 802.1Q VLANs in a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm class1`	Configures an ATM VC class and enters VC-class configuration mode.
Step 4	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-vc-class)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables support for PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs in a VC class. **Note** A VC class can be applied to an ATM interface, subinterface, PVC, or range of PVCs.

Monitoring and Maintaining PPPoE over IEEE 802.1Q VLAN

Perform this task to monitor and maintain PPPoE over VLAN connections.

SUMMARY STEPS

1. **enable**
2. **clear pppoe** {**interface** *type number* [**vc** {[*vpi/*]*vci* | *vc-name*}] [**vlan** *vlan-id*] | **rmac** *mac-address* [**sid** *session-id*] | **all**}
3. **debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number*[**vc** {[*vpi /*]*vci* | *vc-name*}] [**vlan** *vlan-id*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear pppoe** {**interface** *type number* [**vc** {[*vpi/*]*vci* | *vc-name*}] [**vlan** *vlan-id*] | **rmac** *mac-address* [**sid** *session-id*] | **all**} **Example:** `Router# clear pppoe interface fastethernet 0/2 vlan 1`	Clears PPPoE sessions.
Step 3	**debug pppoe** {**data** | **errors** | **events** | **packets**} [**rmac** *remote-mac-address* | **interface** *type number*[**vc** {[*vpi /*]*vci* | *vc-name*}] [**vlan** *vlan-id*]] **Example:** `Router# debug pppoe events interface atm 0/0 vc 1/16 vlan 10`	Displays debugging information for PPPoE sessions.

Configuration Examples for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

- Configuring PPPoE over IEEE 802.1Q VLAN Support on an Ethernet Interface Example, page 136
- Configuring PPPoE over IEEE 802.1Q VLAN Support on ATM PVCs Example, page 137

Configuring PPPoE over IEEE 802.1Q VLAN Support on an Ethernet Interface Example

The following example shows how to configure PPPoE over a range of IEEE 802.1Q VLANs on Fast Ethernet interface 0/0. The VLAN range is configured on the main interface and therefore each VLAN will not use up a separate subinterface.

```
bba-group pppoe PPPOE
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
```

```
 pppoe enable group PPPOE
 exit-vlan-config
```

Configuring PPPoE over IEEE 802.1Q VLAN Support on ATM PVCs Example

The following example shows how to configure an ATM PVC to support PPPoE over a range of IEEE 802.1Q VLANs:

```
bba-group pppoe PPPOEOA
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 10.10.10.10 255.255.255.0
 mtu 1492
interface atm 4/0.10 multipoint
 pvc 10/100
  protocol pppovlan dot1q range 10 30 group PPPOEOA
```

Additional References

The following sections provide references related to the PPPoE Over VLAN Enhancements: Configuration Limit Removal and ATM Support feature.

• Related Documents, page 137

Related Documents

Related Topic	Document Title
ATM PVC configuration	ATM chapter of the Cisco IOS Wide-Area Networking Configuration Guide
PPPoE and PPPoE over IEEE 802.1Q VLAN configuration	Broadband Access: PPP and Routed Bridge Encapsulation chapter of the Cisco IOS Wide-Area Networking Configuration Guide
VLAN range configuration (using subinterfaces)	VLAN Range feature module
ATM PVC and PPPoE configuration commands	Cisco IOS Wide-Area Networking Command Reference

Standards

Standard	Title
IEEE Standard 802.1Q, 1998	*Virtual Bridged Local Area Networks*

MIBs

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

RFCs

RFC	Title
RFC 1483	*Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Technical Assistance

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

Feature Information for PPPoE over VLAN Enhancements Configuration Limit Removal and ATM Support

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

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

Table 8 Feature Information for PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support

Feature Name	Releases	Feature Information
PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support	12.2 (31)SRC 12.3(2)T 12.2(33)SB	The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature provides two enhancements to PPP over Ethernet (PPPoE) over IEEE 802.1Q VLAN functionality: • It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router to 4000 VLANs per interface. • It adds ATM permanent virtual circuit (PVC) support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation. In Cisco IOS Release 12.2(31)SRC, this feature was introduced. In Cisco IOS Release 12.3(2)T, this feature was integrated into the T train. In Cisco IOS Release 12.2(33)SB, support was added for the Cisco IOS 10000 series routers. The following commands were introduced or modified: **clear pppoe** , **debug pppoe**, **pppoe enable**, **protocol pppovlan dot1q**, **vlan-id dot1q**, **vlan-range dot1q**.

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 permanent virtual circuits (PVCs) that are used in supporting broadband access aggregation of PPPoE sessions.

Note This module describes the method to configure PPPoE sessions using profiles. If you have configured your PPPoE sessions using a release of Cisco IOS software earlier than Cisco IOS Release 12.4, see the documentation that corresponds to that release. Although the configuration methods used in Cisco IOS software releases prior to Release 12.4 are supported in Release 12.4, it is recommended that you use the configuration methods described in this module for new configurations and when upgrading to Cisco IOS Release 12.4.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for 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

PPPoE profiles separate the configuration of PPPoE from the configuration of virtual private dialup networks (VPDNs). The legacy method of configuring PPPoE in VPDN groups is permitted, but you cannot configure PPPoE profiles and PPPoE in VPDN groups simultaneously.

Note VPDN is not supported on the Cisco 7600 router in Cisco IOS Release 12.2(33)SRC.

If a PPPoE profile is assigned to a PPPoE port (Ethernet, interface, VLAN, or virtual circuit (VC) class), or ATM range and the profile has not yet been defined, the following restrictions are applicable:

- The port, VC class, or range does not have any PPPoE parameters configured.
- The port, VC class, or range does not use parameters from the global group.

Only PPPoE over 802.1Q VLAN support can be configured without using subinterfaces on the PPPoE server.

ATM support for PPPoE over 802.1Q VLANs can be configured only on the PPPoE server. Individual VLANs that are configured on subinterfaces can be shut down. Individual VLANs that are configured on the main interface cannot be shut down.

A VLAN range can be configured on a main interface at the same time that VLANs outside the range are configured on subinterfaces of the same main interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time.

Note Cisco IOS Release 12.2(33)SRC does not support VCs or ATMs.

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

PPPoE Specification Definition

PPPoE is a specification that defines how a host PC interacts with a 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, Ethernet and PPP, the PPPoE implementation allows users over the Ethernet to share a connection. The 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.

Benefits of PPPoE Profiles

Before the introduction of the use of PPPoE profiles, PPPoE parameters were configured within a VPDN group. Configuring PPPoE in a VPDN group limited PPPoE configuration options because only one PPPoE VPDN group with one virtual template was permitted on a device. The PPPoE Profiles feature provides simplicity and flexibility in PPPoE configuration by separating PPPoE from VPDN configuration. The PPPoE Profiles feature allows multiple PPPoE profiles, each with a different configuration, to be used on a single device.

Note VPDN is not supported on the Cisco 7600 router in Cisco IOS Release 12.2(33)SRC.

Note This module describes the method for configuring PPPoE sessions using profiles. If you have configured your PPPoE sessions using a release of Cisco IOS software earlier than Cisco IOS Release 12.4, see the documentation that corresponds to that release. Although the configuration methods used in Cisco IOS software releases prior to Release 12.4 are supported in Release 12.4, it is recommended that you use the configuration methods described in the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module for new configurations and when upgrading to Cisco IOS Release 12.4.

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 Profile Assignment to a VLAN Without Subinterfaces

Use PPPoE profile assignment to a VLAN without subinterfaces to improve PPPoE over IEEE 802.Q VLAN functionality in the following two ways:

- It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router from 1001 to 4000 VLANs per interface.
- It adds ATM support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation.

Note ATM is not supported on the Cisco 7600 router in Cisco IOS Release 12.2(33)SRC.

To configure PPPoE over 802.1Q VLAN support on an interface rather than a subinterface, and to configure ATM support for PPPoE over 802.1Q VLANs, you should understand the concepts described in the following sections:

- PPPoE over VLAN Configuration Without Using Subinterfaces, page 144
- PPPoE over VLAN Support on ATMs, page 144
- Benefits of PPPoE over VLAN Scaling and ATM Support for PPPoE over VLANs, page 145

PPPoE over VLAN Configuration Without Using Subinterfaces

PPPoE profile assignment to a VLAN without subinterfaces removes the requirement for each PPPoE VLAN to be created on a subinterface. Allowing more than one PPPoE VLAN to be configured on a main interface increases the number of VLANs that can be configured on a router from 1001 to 4000 VLANs per interface.

Individual VLANs or a range of VLANs can be configured on an interface. You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface.

PPPoE over VLAN Support on ATMs

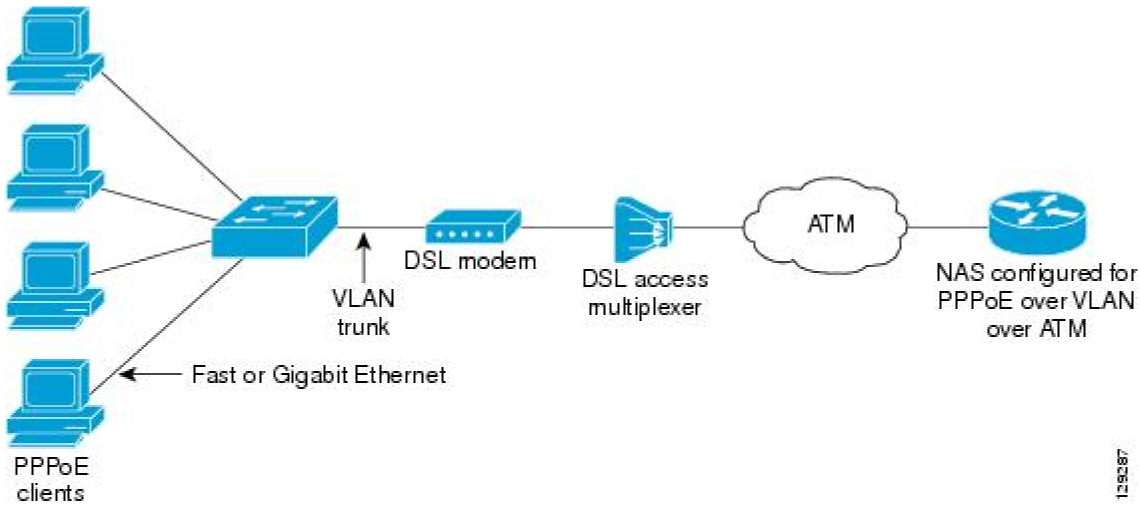
PPPoE profile assignment to a VLAN without subinterfaces enables ATMs to process PPPoE over VLAN packets that use bridged RFC 1483 encapsulation. This capability allows PPPoE traffic from different 802.1Q VLANs to be multiplexed over the same ATM.

The figure below shows a sample network topology that implements PPPoE over VLAN on ATM. In this topology, a service provider is using an Ethernet switch to provide Ethernet service to home users and a single multiplexer to provide the switch with WAN access. The home users use PPPoE to access services on the network access server (NAS). Each port on the switch is assigned a separate VLAN, and the VLANs are trunked over a Fast Ethernet or Gigabit Ethernet interface that is connected to a DSL modem acting as a bridge.

The 802.1Q VLAN-encapsulated traffic coming in from the Ethernet switch trunk is encapsulated in RFC 1483 bridged encapsulation by the DSL modem and sent across the ATM WAN to the NAS. The NAS, which is configured to support PPPoE over VLAN over ATM, will extract the PPPoE packet from the PPPoE over 802.1Q VLAN over RFC 1483 bridged encapsulation and provide PPPoE services to the user.

In the downlink, the NAS sends packets in PPPoE over 802.1Q VLAN over RFC 1483 bridged encapsulation. The DSL modem strips off the RFC 1483 encapsulation and forwards the 802.1Q VLAN packets across the trunk to the switch. The switch then sends the Ethernet packets to the port associated with the 802.1 VLAN ID.

Figure 11 Sample Network Topology for PPPoE over 802.1Q VLAN over ATM



Benefits of PPPoE over VLAN Scaling and ATM Support for PPPoE over VLANs

PPPoE over VLAN scaling and ATM support for PPPoE over VLANs has the following benefits:

- Increases the number of VLANs that can be configured on a router from 1001 to 4000 VLANs per interface by removing the requirement for each PPPoE VLAN to be configured on a subinterface.
- Provides support for PPPoE over VLAN over ATM interfaces using RFC 1483 bridged encapsulation.

Autosense for ATMs

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

Note The Preauthentication with ISDN PRI and Channel-Associated Signalling feature is supported on Subnetwork Access Protocol (SNAP)-encapsulated ATMs only. It is not supported on multiplexer (MUX)-encapsulated.

- Benefits of Autosense for ATMs, page 145

Benefits of Autosense for ATMs

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

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

MAC Address for PPPoEoA

Any change in the usage of MAC addresses will not happen unless it is explicitly configured. This will prevent you from experiencing unexpected behavior resulting from a system change.

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 such as 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 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 interface configured in a BBA group.

When PPPoE and RBE are configured on two separate ATMs on the same DSL, the customer premises equipment (CPE) acts like a pure bridge, bridging from Ethernet to the two ATMs 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 MAC address. 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 146

Benefits of the Configurable MAC Address for PPPoE Feature

Because the Cisco IOS 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, you must define the profile. The profile definition is required as described in the Defining a PPPoE Profile, page 147, and an additional task makes an assignment of the profile to a protocol type.

When assigning a PPPoE profile to a VLAN without a subinterface, choose from the following tasks:

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

- Defining a PPPoE Profile, page 147
- Assigning a PPPoE Profile to an Ethernet Interface, page 149
- Assigning a PPPoE Profile to an ATM, page 150
- Assigning a PPPoE Profile to an ATM Range and Within a Range, page 152
- Assigning a PPPoE Profile to an ATM VC Class, page 155
- Assigning a PPPoE Profile to a VLAN Subinterface, page 157
- Configuring PPPoEoE on a Cisco 7600 SIP-400, page 159
- Enabling PPPoE over IEEE 802.1Q VLAN, page 170
- Enabling an ATM to Support Encapsulated PPPoE over IEEE 802.1Q VLAN, page 172
- Enabling Support for PPPoE over IEEE 802.1Q VLAN in a VC Class, page 173
- Configuring MAC Addresses for PPPoEoA, page 174
- Configuring PPPoE Session Recovery After Reload, page 176
- Monitoring and Maintaining PPPoE Profiles, page 178

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** *vlan-id*
8. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
9. **sessions** {**per-mac**| **per-vc**} **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.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** {*group-name* | **global**} **Example:** `Router(config)# bba-group pppoe 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 a 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.
Step 7	**sessions per-vlan limit** *per-vlan-limit* [**inner** *vlan-id* **Example:** `Router(config-bba-group)# session per-vlan limit 4000 inner 3500`	Sets the maximum number of PPPoE sessions permitted per VLAN in a PPPoE profile.
Step 8	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** `Router(config-bba-group)# sessions per-vc limit threshold 8`	Sets the maximum number of PPPoE sessions permitted on a VC in a PPPoE profile, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

	Command or Action	Purpose
Step 9	**sessions** {**per-mac**| **per-vc**} **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 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`	Exits the configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an Ethernet Interface

Perform this task to assign a PPPoE profile to an Ethernet interface.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *number* **Example:** `Router(config)# interface ethernet 2/0`	Specifies an 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 an Ethernet interface or subinterface. **Note** If a PPPoE profile is not assigned to the interface by using the **group** *group-name* option, the interface will use the global PPPoE profile.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Exits the configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to an ATM

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [*.subinterface-number* {**multipoint** | **point-to-point**}]
4. **pvc** [**name**] *vpi/vci*[**ilmi** | **l2transport** | **qsaal**]
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* [.*subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters subinterface configuration mode.
Step 4	**pvc** [**name**] *vpi/vci*[**ilmi** | **l2transport** | **qsaal**] **Example:** `Router(config-subif)# 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 the ATMs.
		or
		Configures PPPoA/PPPoE autosense on the MUX- and SNAP-encapsulated ATM PVCs.
		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.

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

Assigning a PPPoE Profile to an ATM Range and Within a Range

Perform this task to assign a PPPoE profile to an ATM range and within a range.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [.*subinterface-number* {**multipoint** | **point-to-point**}]
4. **range** [*range-name*] **pvc** [*start-vpi*/]*start-vci*
5. **protocol pppoe** [**group** *group-name*]
6. **pvc-in-range** [-*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.

	Command or Action	Purpose
Step 3	**interface atm** *number* [.*subinterface-number* {**multipoint** | **point-to-point**}] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters subinterface configuration mode.

Step 4	**range** [*range-name*] **pvc** [*start-vpi*/]*start-vci*
	
	Example:
	
	[*end-vpi*/]*end-vci*
	
	Example:
	
	`Router(config-subif)# range range-pppoa-1 pvc`
	
	Example:
	
	`100 4/199`
		Defines a range of ATM profiles 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 ATMs.
		
		or
		
		Configures PPPoA/PPPoE autosense.
		
		Note If a PPPoE profile is not assigned to the range by using the **group** *group-name* option, the ATMs in the range will use the global PPPoE profile.

Step 6	**pvc-in-range** [*-name*] [[*vpi* /]*vci*] **Example:** `Router(config-if-atm-range)# pvc-in-range 1 3/104`	Defines an individual ATMs within a range and enters 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 group within a range.
		or
		Configures PPPoA/PPPoE autosense.
		Note If a PPPoE profile is not assigned to the range by using the **group** *group-name* option, the ATMs in the range will use the global PPPoE profile.

Step 8	**end** **Example:** `Router(config-if-atm-range-)# end`	(Optional) Exits the 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 PPPoA/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 the configuration mode and returns to privileged EXEC mode.

Assigning a PPPoE Profile to a VLAN Subinterface

Perform this task to assign a PPPoE profile to a VLAN subinterface.

Note This configuration method requires the use of subinterfaces. One subinterface supports one VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface range** {**fastethernet** *interfacenumber - interfacenumber* | **gigabitethernet** *interfacenumber - interfacenumber* | **loopback** *number*| **tunnel** *number*| **port-channel** *number* | **vlan** *number* | **macro** *keyword*}
4. **encapsulation dotlq** *vlan-id* **second-dot1q** {**any** | *vlan-id*} [**native**]
5. **protocol pppoe** [**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 range** {**fastethernet** *interfacenumber - interfacenumber* | **gigabitethernet** *interfacenumber - interfacenumber* | **loopback** *number*| **tunnel** *number*| **port-channel** *number* | **vlan** *number* | **macro** *keyword*} **Example:** `Router(config)# interface range fastethernet 5/1.1 - fastethernet 5/1.4`	Assigns a subinterface to an interface and enters interface range configuration mode.
Step 4	**encapsulation dotlq** *vlan-id* **second-dot1q** {**any** | *vlan-id*} [**native**] **Example:** `Router(config-if-range)# encapsulation dot1q 301`	Sets the encapsulation method used by the interface.
Step 5	**protocol pppoe** [**group** *group-name*] **Example:** `Router(config-if-range)# protocol pppoe group two`	Enables PPPoE sessions to be established.

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

Configuring PPPoEoE on a Cisco 7600 SIP-400

PPP provides a standard method of communicating to peers over a point-to-point link. An Ethernet link provides multipoint communication between multiple peers. PPPoE allows point-to-point communication across multipoint Ethernet links.

The PPPoE over Ethernet interface (PPPoEoE) enables the Cisco 7600 series router with a Cisco 7600 SIP-400 to tunnel and terminate Ethernet PPP sessions over Ethernet links. The PPPoE over IEEE 802.1Q VLANs feature enables the router to tunnel and terminate Ethernet PPP sessions across VLAN links. IEEE 802.1Q encapsulation is used to interconnect a VLAN-capable router with another VLAN-capable networking device. The packets on the 802.1Q link contain a standard Ethernet frame and the VLAN information associated with that frame.

PPPoEoE on Cisco 7600 SIP-400 supports the following features:

- PPPoE discovery packets (rate-limited), PPPoE PPP control packets, and PPPoE PPP IP data packets provide a per-user session on an Ethernet interface.
- PPPoE is supported on main interfaces, 802.1q and QinQ access interfaces, and VLAN ranges (802.1q ranges and QinQ inner ranges).
- 8000 PPPoE sessions are supported.
- PPPoE and IP sessions can be configured on the same subinterface.

Restrictions

- PPPoA and any PPP feature on ATM interfaces are not supported.
- Ambiguous VLANs and a range of VLANs for IP session interfaces are not supported. However, a range of VLANs is supported for PPPoE-configured interfaces.
- Negotiated maximum transmission unit (MTU) value can only be 1492 or 1500 bytes.
- If the **ip tcp adjust-mss** command is used, the only value supported is 1468.
- PPPoE can be configured only on subinterfaces.
- Layer 2 Tunnel Protocol (L2TP) tunneling of PPPoE sessions is not supported.

Configuration Tasks for PPPoE over Ethernet

To configure PPPoE over Ethernet, perform the following tasks:

- Creating an Ethernet Interface and Enabling PPPoE, page 162
- Configuring a BBA Group to Establish PPPoE Sessions, page 163
- Tasks for Configuring PPPoE over 802.1Q VLANs on a Cisco 7600 Router with a SIP-400, page 166

Configuring a Virtual Template Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**Interface virtual-template** *number* [**type** [**ethernet** | **serial** | **tunnel**]] **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip unnumbered ethernet** *number* **Example:** `Router(config-if)# ip unnumbered ethernet 3/1`	Enables IP without assigning a specific IP address on the LAN.
Step 5	**mtu** *bytes* **Example:** `Router(config-if)# mtu bytes`	(Optional) Sets the maximum MTU size for the interface. • Valid range for the MTU size is 1492 or 1500.
Step 6	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables PPP authentication on the virtual template interface.
Step 7	**ppp ipcp ip address required** **Example:** `Router(config-if)# ppp ipcp ip address required`	Prevents a PPP session from being set up without a valid address being negotiated. This command is required for legacy dialup and DSL networks.
Step 8	end **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Examples

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

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

Monitoring Virtual Access Interface

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created. You cannot use the command-line to directly create or configure a VAI. Perform this task to monitor the VAI and free the memory for other dial-in uses.

SUMMARY STEPS

1. **enable**
2. **show interfaces virtual-access** *number* **[configuration]**
3. **clear interface virtual-access** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interfaces virtual-access** *number* **[configuration]** **Example:** `Router# show interfaces virtual-access 3`	Displays the status, traffic data, and configuration information about a specified active VAI that was created using a virtual template interface. • The **configuration** keyword restricts output to configuration information.
Step 3	**clear interface virtual-access** *number* **Example:** `Router# clear interface virtual-access 3`	Tears down the live sessions and frees the memory for other client users.

Examples

The following example shows how to display the active VAI configuration:

```
Router# show interfaces virtual-access 1.1 configuration
!
interface virtual-access1.1
if vrf forwarding vrf-1
ip unnumbered Loopback1
no ip proxy-arp
peer default ip address pool vrf-1
ppp authentication chap
end
```

Note Virtual-access 1.1 is a PPPoE subinterface.

Creating an Ethernet Interface and Enabling PPPoE

Perform this task to create an Ethernet interface and enable PPPoE on it.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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`	Creates an Ethernet interface and enters GigabitEthernet interface configuration mode.
Step 4	**pppoe enable** [**group** *group-name* **Example:** `Router(config-if)# pppoe enable group1`	Enables PPPoE and allows PPPoE sessions to be created through that interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Configuring a BBA Group to Establish PPPoE Sessions

Note Cisco IOS Release 12.2(33)SRC does not support the configuration of broadband aggregation (BBA) groups using RADIUS. You must configure BBA groups manually.

Perform this task to configure a BBA group to establish PPPoE sessions and link it to the appropriate virtual template interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *name*
4. **virtual-template** *template-number*
5. **sessions per-mac limit** *per-mac-limit*
6. **sessions max limit** *number-of-sessions* [**threshold** *threshold-value*
7. **sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*]
8. **exit**
9. **interface** *type number*
10. **encapsulation dot1q** *vlan-id* s**econd-dot1q** {**any** | *vlan-id* | *vlan-id-vlan-id*[,*vlan-id-vlan-id*]}
11. **protocol pppoe group** *group-name*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**bba-group pppoe** *name* **Example:** `Router(config)# bba-group pppoe name`	Configures a BBA group to be used to establish PPPoE sessions and enters BBA group configuration mode.. The *name* identifies the BBA group. You can have multiple BBA groups.

	Command or Action	Purpose
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	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-group)# sessions per-mac limit 100`	(optional) Specifies the maximum number of sessions per MAC address for each PPPoE port that uses the group.
Step 6	**sessions max limit** *number-of-sessions* [**threshold** *threshold-value* **Example:** `Router(config-bba-group)# sessions max limit 32000` **Example:**	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. This command applies only to the global profile.
Step 7	**sessions per-vc limit** *per-vc-limit* [**threshold** *threshold-value*] **Example:** **Example:** `Router(config-bba-group)# sessions per-vc limit 2000` **Example:**	(Optional) Sets the maximum number of PPPoE sessions allowed per VC session limit in a PPPoE profile.
Step 8	**exit** **Example:** `Router(config-bba)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 9	**interface** *type number* **Example:** `Router(config)# interface atm 2/0`	Specifies the interface to which you want to attach the BBA group and enters interface configuration mode.
Step 10	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id-vlan-id*[,*vlan-id-vlan-id*]} **Example:** `Router(config-if)#encapsulation dot1q vlan-id`	Enables IEEE 802.1Q encapsulation on traffic on a specifiedsubinterface in a VLAN. • Specify the VLAN identifier.
Step 11	**protocol pppoe group** *group-name* **Example:** `Router(config-if)#protocol pppoe group group-name`	Attaches the BBA group to the VLAN.
Step 12	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode.

Tasks for Configuring PPPoE over 802.1Q VLANs on a Cisco 7600 Router with a SIP-400

PPPoE over IEEE 802.1Q VLANs enables the Cisco 7600 series router with a SIP-400 to support PPPoE over IEEE802.1Q encapsulated VLAN interfaces. IEEE 802.1Q encapsulation is used to interconnect a VLAN-capable router with another VLAN-capable networking device. The packets on the 802.1Q link contain a standard Ethernet frame and the VLAN information associated with that frame. Perform the following tasks to configure PPPoE on a Cisco 7600 router with a SIP-400:

Note PPPoE is disabled by default on a VLAN.

Configuring a Virtual Template

Before configuring PPPoE on an IEEE 802.1Q VLAN interface, configure a virtual template. See the Configuring a Virtual Template Interface, page 160.

- Creating an Ethernet 802.1Q Encapsulated Subinterface and Enabling PPPoE, page 166
- Verifying PPPoE over Ethernet, page 168
- Clearing PPPoE Sessions, page 169

Creating an Ethernet 802.1Q Encapsulated Subinterface and Enabling PPPoE

Creating an Ethernet 802.1Q Encapsulated Subinterface and Enabling PPPoE

Perform this task to create an Ethernet 802.1Q interface and enable PPPoE on it.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot* / *subslot* / *port*
4. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*} [**native**]
5. **exit**
6. **bba-group pppoe** {*bba-group-name* | **global**}
7. **pppoe enable pppoe enable** [**group** group-name]
8. **pppoe max-sessions** *number*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot* / *subslot* / *port* **Example:** `Router(config)# interface gigabitethernet 0/2/1`	Creates a Gigabit Ethernet subinterface and enters subinterface configuration mode.
Step 4	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*} [**native**] **Example:** `Router(config-subif)# encapsulation dot1q second-dot1q 20`	Enables IEEE802.1Q encapsulation on a specified subinterface in VLANs.
Step 5	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode.

	Command or Action	Purpose
Step 6	**bba-group pppoe** {*bba-group-name* | **global**} **Example:** `Router(config)# bba-group pppoe group1`	Enters BBA group configuration mode.
Step 7	**pppoe enable pppoe enable** [**group** group-name] **Example:** `Router(config-bba)# pppoe enable group1`	Enables PPPoE and allows PPPoE sessions to be created through the specified subinterface.
Step 8	**pppoe max-sessions** *number* **Example:** `Router(config-bba)# pppoe max-sessions 23`	Specifies the maximum number of PPPoE sessions that can be terminated on this router from all interfaces.
Step 9	**end** **Example:** `Router(config-bba)#` **end**	Exits BBA group configuration mode.

Verifying PPPoE over Ethernet

Perform this task to verify PPPoEoE.

SUMMARY STEPS

1. **enable**
2. **show pppoe session all**
3. **show pppoe session packets**
4. **show pppoe summary**

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	**show pppoe session all** **Example:** `Router# show pppoe session all`	Displays PPPoE session information for each session ID.
Step 3	**show pppoe session packets** **Example:** `Router# show pppoe session packets`	Displays PPPoE session statistics.
Step 4	**show pppoe summary** **Example:** `Router# show pppoe summary`	Displays a summary of PPPoE session information.

Clearing PPPoE Sessions

Perform this task to clear the PPPoE sessions.

SUMMARY STEPS

1. **enable**
2. **clear pppoe all**
3. **clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}]
4. **clear pppoe rmac** *mac-address* [**sid** *session-id*]
5. **clear pppoe interface** *type number* [**vlan** *vlan- number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear pppoe all** **Example:** `Router# clear pppoe all`	Clears all PPPoE sessions.

	Command or Action	Purpose
Step 3	**clear pppoe** {**interface** *type number* [**vc** {[*vpi*/]*vci* | *vc-name*}] **Example:** `Router# clear pppoe interface`	Clears all PPPoE sessions on a physical interface or subinterface.
Step 4	**clear pppoe rmac** *mac-address* [**sid** *session-id*] **Example:** `Router# clear pppoe rmac sid`	Clears PPPoE sessions from a client host MAC address.
Step 5	**clear pppoe interface** *type number* [**vlan** *vlan- number*] **Example:** `Router# clear pppoe interface ATM 2/0 vlan 200`	Clears sessions from a specific VLAN.

Enabling PPPoE over IEEE 802.1Q VLAN

Perform this task to enable PPPoE over IEEE 802.1Q VLAN support on a main Ethernet interface.

The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature removes the requirement for each PPPoE VLAN to be created on a subinterface. Allowing more than one PPPoE VLAN to be configured on a main interface increases the number of VLANs that can be configured on a router from 1001 to 4000 VLANs per interface.

Individual VLANs or a range of VLANs can be configured on an interface. You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **vlan-id dot1q** *vlan-id*
   -
   -
   - **vlan-range dot1q** *start-vlan-id end-vlan-id*
5. **pppoe enable** [**group** *group-name*]
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** *type number* **Example:** `Router(config)# interface fastethernet 0/2`	Specifies the interface to be configured and enters interface configuration mode.

Step 4	Do one of the following:
	
	• **vlan-id dot1q** *vlan-id*
	•
	•
	• **vlan-range dot1q** *start-vlan-id end-vlan-id*
	
	Example:
	
	Example:
	
	`Router(config-if)# vlan-id dot1q 0`
	
	Example:
	
	Example:
	
	`Router(config-if)# vlan-range dot1q 0 60`
		Enables IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface and enters VLAN range configuration mode.
		
		or
		
		Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface and enters VLAN range configuration mode.

	Command or Action	Purpose
Step 5	**pppoe enable** [**group** *group-name*] **Example:** `Router(config-if-vlan-range)# pppoe enable group pppoe1`	Enables PPPoE sessions over a specific VLAN or a range of VLANs.
Step 6	**end** **Example:** `Router(config-if-vlan-range)# end`	Exits VLAN range configuration mode.

Enabling an ATM to Support Encapsulated PPPoE over IEEE 802.1Q VLAN

Perform the following task to enable an ATM to support encapsulated PPPoE over IEEE 802.1Q VLAN traffic. The PPPoE over VLAN Enhancements: Configuration Limit Removal and ATM Support feature enables ATMs to process PPPoE over VLAN packets that use bridged RFC 1483 encapsulation. This capability allows PPPoE traffic from different 802.1Q VLANs to be multiplexed over the same ATM.

For more information, see the PPPoE over VLAN Support on ATMs, page 144.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* **.** *subinterface-number* {**multipoint** | **point-to-point**}
4. **pvc** [*name*] *vpi* / *vci*
5. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]
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.

	Command or Action	Purpose
Step 3	**interface atm** *number* **.** *subinterface-number* {**multipoint** | **point-to-point**} **Example:** `Router(config)# interface atm 2/0.1 multipoint`	Configures an ATM multipoint subinterface and enters subinterface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **Example:** `Router(config-subif)# pvc name1 0/60`	Configures a VC and enters ATM PVC configuration mode.
Step 5	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-if-atm-vc)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs on an ATM.
Step 6	**end** **Example:** `Router(config-if-atm-vc)# end`	Exits ATM PVC configuration mode.

Enabling Support for PPPoE over IEEE 802.1Q VLAN in a VC Class

Perform the following task to enable support for PPPoE over IEEE 802.1Q VLANs in a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *name* **Example:** `Router(config)# vc-class atm class1`	Configures an ATM VC class and enters ATM VC class configuration mode.
Step 4	**protocol pppovlan dot1q** {*vlan-id* | *start-vlan-id end-vlan-id*} [**group** *group-name*] **Example:** `Router(config-vc-class)# protocol pppovlan dot1q 0 50 group pppoe1`	Enables support for PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs in a VC class. **Note** A VC class can be applied to an ATM interface, subinterface, or range of ATMs.

Configuring MAC Addresses for PPPoEoA

You can configure the MAC address on ATMs in a BBA group to use a different MAC address for PPP over Ethernet over ATM (PPPoEoA).

Perform this task to configure different MAC addresses on PPPoEoA and enable the aggregation router to bridge packets from Ethernet to the appropriate MAC addresses..

A BBA group profile should already exist. The BBA group commands are used to configure broadband access on aggregation and client devices that use PPPoA, PPPoE, and Routed Bridge Encapsulation (RBE).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** {*bba-group-name* | **global**}
4. **mac-address** {**autoselect** | *mac-address*}
5. **exit**
6. **show pppoe session**
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	**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. • **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	**exit** **Example:** `Router(config-bba-group)# exit`	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.
Step 7	end **Example:** `Router# end`	Exits privileged EXEC mode.

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 CPE device, a PPPoE session will pause 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. **virtual-template** *template-number*
5. **sessions auto cleanup**
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 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	**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 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.

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

• Troubleshooting Tips, page 178

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.

	Command or Action	Purpose
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 0/1.0`	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

PPPoE Profiles Configuration Example

The following example shows how to configure the three PPPoE profiles: vpn1, vpn2, and a global PPPoE profile. The profiles vpn1 and vpn2 are assigned to VC classes, VLANs, and ranges. Any Ethernet interface, VLAN, 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.

Note The order in which the commands are configured can be changed.

```
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain vpn1
 initiate-to ip 209.165.200.225 priority 1
 local name NAS1-1
!
```

```
vpdn-group 2
 request-dialin
  protocol l2tp
  domain vpn2
 initiate-to ip 209.165.201.1 priority 1
 local name NAS1-2
!
virtual-template 1 pre-clone 20
virtual-template 2 pre-clone 20
!
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
  sessions per-mac limit 2
  sessions per-vc limit 8
!
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-mac limit 1
 sessions per-vc limit 2
!
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 Loopback 1
 ip address 209.165.201.1 255.255.255.0
!
interface ATM 1/0.10 multipoint
range range-pppoe-1  100 109
  protocol pppoe group vpn1
 !
interface ATM 1/0.20 multipoint
 class-int class-pppox-auto
  0/200
  encapsulation aal5autoppp virtual-template 1
 !
  0/201
 !
  0/202
  encapsulation aal5autoppp virtual-template 1 group vpn2
 !
  0/203
  class-vc class-pppoe-global
 !
!
interface Ethernet 2/3.1
 encapsulation dot1Q 1
 pppoe enable group vpn1
!
interface Ethernet 2/3.2
 encapsulation dot1Q 2
 pppoe enable group vpn2
!
interface ATM 6/0.101 point-to-point
 ip address 209.165.202.129 255.255.255.0
  0/101
 !
interface ATM 6/0.102 point-to-point
 ip address 209.165.201.1 255.255.255.0
```

```
  0/102
 !
interface virtual-template 1
 ip unnumbered loopback 1
 no logging event link-status
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
!
interface virtual-template 2
 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 10.10.1.1 10.10.1.250
ip local pool pool-2 10.10.2.1 10.10.2.250
!
```

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

In the following example, neither address autoselect nor a MAC address is configured on the BBA group, and the MAC address is not configured on the ATM interface (the default condition). The **show pppoe session** command is used to confirm that the MAC address of the PPPoEoA session is the burned-in MAC address of the ATM interface.

```
bba-group pppoe one
 virtual-template 1
interface ATM 3/0
 no ip address
 no ip route-cache
no atm ilmi-keepalive
!
interface ATM 3/0.1 multipoint
 no ip route-cache
  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  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).
```

Address Autoselect Configured and MAC Address Not Configured Example

The following example shows how to configure address autoselect in the BBA group. 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 ATM 3/0
 no ip address
 no ip route-cache
```

```
 no atm ilmi-keepalive
!
interface ATM 3/0.1 multipoint
 no ip route-cache
  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  ATM3/0.1                 1  Vi2.1
PTA
                0008.7c55.a05b  VC:  1/50                   UP
LocMAC = burned in mac-address of ATM interface + 7 (0008.7c55.a05b)
```

PPPoE over 802.1Q VLAN Support on an Ethernet Interface Example

The following example shows how to configure PPPoE over a range of 802.1Q VLANs on FastEthernet interface 0/0. The VLAN range is configured on the main interface, and therefore each VLAN will not use up a separate subinterface.

```
bba-group pppoe PPPOE
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 209.165.201.1 255.255.255.0
 mtu 1492
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
  pppoe enable group PPPOE
  exit-vlan-config
```

PPPoE over 802.1Q VLAN Support on ATMs Example

The following example shows how to configure an ATM to support PPPoE over a range of 802.1Q VLANs:

```
bba-group pppoe PPPOEOA
 virtual-template 1
 sessions per-mac limit 1
interface virtual-template 1
 ip address 209.165.202.129 255.255.255.0
 mtu 1492
interface atm 4/0.10 multipoint
  10/100
  protocol pppovlan dot1q 0 50 group PPPOEOA
```

MAC Address Configured on the ATM Interface Example

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

```
bba-group pppoe one
 virtual-template 1
interface ATM 3/0
 mac-address 0001.0001.0001
 no ip address
```

```
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM 3/0.1 multipoint
 no ip route-cache
  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  ATM3/0.1                 1  Vi2.1
PTA
                0001.0001.0001  VC:  1/50                   UP
LocMAC = configured mac-address on atm interface(0001.0001.0001).
```

MAC Address Configured on the BBA Group Example

The following example shows how to configure the MAC address 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 ATM 3/0
 mac-address 0001.0001.0001
 no ip address
 no ip route-cache
 no atm ilmi-keepalive
!
interface ATM 3/0.1 multipoint
 no ip route-cache
  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  ATM3/0.1                 1  Vi2.1
PTA
                0002.0002.0002  VC:  1/50                   UP
LocMac(Mac address of PPPoEoA session) is mac-address specified on bba-group one
(0002.0002.0002)
```

PPPoE Session Recovery After Reload Example

The following example shows how the router attempts to recover failed PPPoE sessions in the ATM range called "range-pppoe-1":

```
bba-group pppoe group1
 virtual-template 1
 sessions auto cleanup
!
interface ATM1/0.10 multipoint
 range range-pppoe-1  100 109
  protocol pppoe group group1
!
interface virtual-template 1
 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 PVC or VLAN configured on an 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.

Note L2TP is not supported on the Cisco 7600 router in Cisco IOS Release 12.2(33)SRC.

- If you want to configure the transfer upstream of the Point-to-Point Protocol over X (PPPoX, where X designates a family of encapsulating communications protocols such as pppoe, pppoa, pppoeoa, pppoeovlan implementing PPP), see the "Configuring Upstream Connections Speed Transfer" module.
- If you want to use SNMP to monitor PPPoE sessions, see the "Monitoring PPPoE Sessions with SNMP" module.
- If you want to identify a physical subscribe line for RADIUS communication with a RADIUS server, see the "Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module.
- If you want to configure a Cisco Subscriber Service Switch, see the "Configuring Cisco Subscriber Service Switch Policies" module.

Additional References

The following sections provide references related to the Providing Protocol Support for Broadband Access Aggregation of PPPoE Session feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	"Understanding Broadband Access Aggregation" module in *Cisco IOS Broadband and DSL Configuration Guide*
Tasks for preparing for broadband access aggregation	"Preparing for Broadband Access Aggregation" module in the *Cisco IOS Broadband and DSL Configuration Guide*
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Related Topic	Document Title
Establishing PPPoE session limits for sessions on a specific permanent virtual circuit or VLAN configured on an L2TP access concentrator	"Establishing PPPoE Session Limits per NAS Port" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
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" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
Enabling an L2TP access concentrator to relay active discovery and service selection functionality for PPPoE over an L2TP control channel to an L2TP LNS or tunnel switch	" Enabling PPPoE Relay Discovery and Service Selection Functionality" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
Configuring the transfer upstream of the PPPoX session speed value	" Configuring Upstream Connections Speed Transfer" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
Using SNMP to monitor PPPoE sessions	"Monitoring PPPoE Sessions with SNMP" in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
Identifying a physical subscribe line for RADIUS communication with a RADIUS server	" Identifying a Physical Subscriber Line for RADIUS Access and Accounting" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*
Configuring a Cisco Subscriber Service Switch	"Configuring Cisco Subscriber Service Switch Policies" module in *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*

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 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 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 Providing Protocol Support for Broadband Access Aggregation for 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 9 Feature Information for Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions

Feature Name	Software Releases	Feature Configuration Information
Configurable MAC Address for PPPoE	12.3(11)T	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). The following commands were introduced or modified: **bba-group ppoe**, **mac-address**.
Configuration Limit Removal and ATM Support	12.3(2)T	The Configuration Limit Removal and ATM Support feature provides two enhancements to PPP over Ethernet (PPPoE) over IEEE 802.1Q VLAN functionality: • It removes the requirement for each PPPoE VLAN to be created on a subinterface. Removal of this requirement increases the number of VLANs that can be configured on a router from 1001 to 4000 VLANs per interface. • It adds ATM support for PPPoE over VLAN traffic that uses bridged RFC 1483 encapsulation. The following commands were introduced or modified: **encapsulation dot1q**, **interface atm**, **interface range, protocol pppoe**, **pppoe enable**, **protocol pppoe**, **vlan-id dot1q**, **vlan dot1q**.

Feature Name	Software Releases	Feature Configuration Information
PPPoA/PPPoE Autosense for ATMs	12.1(1)DC 12.2(4)T 12.2(4)T3	The PPPoA/PPPoE Autosense for ATMs feature enables a router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATMsessions and to create virtual access based on demand for both PPP types. The following commands were introduced or modified: **encapsulation aal5 auto, interface ATM**, **ppp virtual-template**, **protocol pppoe**, **pvc-in-range**, **range**.
PPPoE Connection Throttling	12.2 (15)T 12.2(33)SRC	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 Profiles	12.2(15)T	The PPPoE Profiles feature configures PPP over Ethernet profiles that contain configuration information for a group of PPPoE sessions.
PPPoE Session Recovery After Reload	12.3(2)T 12.2(33)SRC	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.

Feature Name	Software Releases	Feature Configuration Information
VLAN Range	12.0(7)XE 12.1(5)T 12.2(2)DD 12.2(4)B 12.2(8)T 12.2(13)T	The VLAN Range feature can be used to group VLAN subinterfaces so that any command entered in a group applies to every subinterface within the group. This capability simplifies configurations and reduces command parsing.

PPPoE Client DDR Idle-Timer

The PPPoE Client DDR Idle-Timer feature supports the dial-on-demand routing (DDR) interesting traffic control list functionality of the dialer interface with a PPP over Ethernet (PPPoE) client, but also keeps original functionality (PPPoE connection up and always on after configuration) for those PPPoE clients that require it.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for PPPoE Client DDR Idle-Timer

Before configuring the PPPoE Client DDR Idle-Timer feature, you must understand the concept of DDR interesting packets and access control lists and PPPoE Stage Protocols. See the Prerequisites for PPPoE Client DDR Idle-Timer, page 191 for links to the documents describing these concepts.

Information About PPPoE Client DDR Idle-Timer

DDR Functionality and the PPPoE Client

Before Cisco IOS Release 12.2(13)T, the DDR interesting traffic control list functionality of the dialer interface was not supported for PPPoE. However, the PPPoE Client DDR Idle-Timer feature, available as part of Cisco IOS Release 12.2(13)T, now supports this DDR functionality for a PPPoE client.

Protocol access lists and dialer access lists are central to the operation of DDR. Access lists are used as the screening criteria for determining when to initiate DDR calls. All packets are tested against the dialer access list. Packets that match a permit entry are deemed interesting. Packets that do not match a permit entry or that do match a deny entry are deemed uninteresting. When a packet is found to be interesting, either the dialer idle timer is reset (if the line is active) or a connection is attempted (assuming the line is available but not active). If a tested packet is deemed uninteresting, it will be forwarded if it is intended for a destination known to be on a specific interface and the link is active. However, such a packet will not initiate a DDR call and will not reset the idle timer. If dialer idle timer expires, the dialer interface calls a PPPoE function to tear down the connection.

A new command, **pppoe-client dial-pool-number**, allows configuring a DDR interesting traffic control list for PPPoE connections, but also keeps original connection functionality for those PPPoE clients that require it. If you do not require DDR, the PPPoE connection will be up and always on after configuration. If you do require DDR functionality, the connection will be brought up when interesting traffic comes in from the LAN interface and brought down after the dialer idle timer expires. Interesting traffic that comes from WAN interface will only reset the dialer idle timer.

Protocol access lists and dialer access lists have already been implemented in the dialer interface for the operation of DDR. For a PPPoE client, access lists are used as the screening criteria for determining if PPPoE Discovery initiation or a dialer idle timer reset is needed. But a protocol access list is not required for this feature; it depends on your network needs. An access-list can be configured and associated with dialer-list, or you can configure only the dialer list.

All packets destined to the dialer interface are tested against the dialer access list. Packets that match a permit entry are deemed interesting. Packets that do not match a permit entry or that do match a deny entry are deemed uninteresting. When a packet is found to be interesting, the dialer idle timer will be reset if the PPPoE session has already been set up, or a PPPoE Discovery will be attempted if there is no PPPoE session. If a tested packet is deemed uninteresting, it will not initiate PPPoE Discovery and will not reset the idle timer.

How to Configure PPPoE Client DDR Idle-Timer

Configure the PPPoE Client DDR Idle-Timer on an ATM PVC Interface

To configure the PPPoE client DDR idle-timer in interface-ATM-VC configuration mode, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface atm** *atm-interface-number*
4. **pvc** *vpi/vci*
5. **pppoe-client dial-pool-number** *number* [**dial-on-demand**]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *atm-interface-number* **Example:** `Router# interface atm 2/0`	Configures an ATM interface type and enters interface configuration mode.
Step 4	**pvc** *vpi/vci* **Example:** `Router(config-if)# pvc 2/100`	Creates an ATM permanent virtual circuit (PVC) and enters interface-ATM-VC configuration mode.
Step 5	**pppoe-client dial-pool-number** *number* [**dial-on-demand**] **Example:** `Router(config-if-atm-vc)# pppoe-client dial-pool-number 1 dial-on-demand`	Configures DDR interesting traffic control list functionality of the dialer interface with a PPPoE client. • The optional **dial-on-demand** keyword enables DDR functionality on the PPPoE connection.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits the configuration mode. • Enter the **exit** command at each configuration mode to leave that mode.

- What to Do Next, page 194

What to Do Next

To support DDR functionality for the PPPoE client, DDR functionality must be configured. See the Configure the Dialer Interface, page 195 for the steps to do this.

Configure the PPPoE Client DDR Idle-Timer on an Ethernet Interface

To configure the PPPoE client DDR idle-timer on an Ethernet interface, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface ethernet** *ethernet-number*
4. **pppoe enable**
5. **pppoe-client dial-pool-number** *number* [**dial-on-demand**]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface ethernet** *ethernet-number* **Example:** `Router# interface ethernet 1`	Configures an Ethernet interface and enters interface configuration mode.
Step 4	**pppoe enable** **Example:** `Router(config-if)# pppoe enable`	Enables PPPoE sessions on an Ethernet interface.
Step 5	**pppoe-client dial-pool-number** *number* [**dial-on-demand**] **Example:** `Router(config-if)# pppoe-client dial-pool-number 1 dial-on-demand`	Configures DDR interesting traffic control list functionality of the dialer interface with a PPPoE client. • The optional **dial-on-demand** keyword enables DDR functionality on the PPPoE connection.
Step 6	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits the configuration mode. • Enter the **exit** command at each configuration mode to leave that mode.

- What to Do Next, page 195

What to Do Next

To support DDR functionality for the PPPoE client, DDR functionality must be configured. See the Configure the Dialer Interface, page 195 section for the steps to do this.

Configure the Dialer Interface

To configure the dialer interface (required when using the **pppoe-client dial-pool-number** command), you must also configure the following commands:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface dialer** *dialer-rotary-group-number*
4. **dialer idle-timeout** *seconds* [**inbound** | **either**]
5. **dialer hold-queue** *packets* [**timeout** *seconds*]
6. **dialer-group** *group-number*
7. **exit**
8. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface dialer** *dialer-rotary-group-number* **Example:** `Router# interface dialer 1`	Defines a dialer rotary group and enters interface configuration mode.
Step 4	**dialer idle-timeout** *seconds* [**inbound** | **either**] **Example:** `Router(config-if)# dialer idle-timeout 180 either`	Specifies the duration of idle time before a line is disconnected. • **inbound** --Only inbound traffic will reset the idle timeout. • **either** --Both inbound and outbound traffic will reset the idle timeout.
Step 5	**dialer hold-queue** *packets* [**timeout** *seconds*] **Example:** `Router(config-if)# dialer hold-queue 100`	Allows interesting outgoing packets to be queued until a modem connection is established. • **timeout** --Amount of time, in seconds, to queue the packets.

	Command or Action	Purpose
Step 6	**dialer-group** *group-number* **Example:** `Router(config-if)# dialer-group 1`	Controls access by configuring an interface to belong to a specific dialing group.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Leaves interface configuration mode and returns to global configuration mode.
Step 8	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ip permit`	Defines a DDR dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. • **permit** and **deny**--Configure access permissions. • **list** --Specifies that an access list will be used for defining a granularity finer than an entire protocol.

Configuration Examples for PPPoE Client DDR Idle-Timer

This section provides configuration examples to match the identified configuration tasks in the previous sections. The dialer interface configurations for each interface type required by the **pppoe-client dial-pool-number** command are included in the following client configuration examples:

- PPPoEoA Client Configuration Example, page 197
- PPPoEoE Client Configuration Example, page 198

PPPoEoA Client Configuration Example

The following example shows how to configure the PPPoE client DDR idle-timer on an ATM PVC interface:

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface ATM2/0
 pvc 2/100
  pppoe-client dial-pool-number 1 dial-on-demand
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
```

```
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 180 either
 dialer hold-queue 100
 dialer-group 1
!
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

PPPoEoE Client Configuration Example

The following example shows how to configure the PPPoE client DDR idle-timer on an Ethernet interface:

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface Ethernet1
 pppoe enable
 pppoe-client dial-pool-number 1 dial-on-demand
!
interface Dialer1
 ip address negotiated
ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 180 either
 dialer hold-queue 100
 dialer-group 1
!
dialer-list 1 protocol ip permit
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
DDR interesting packets and access control lists	*Cisco IOS Dial Technologies Configuration Guide* , Release 12.2. See the section "Configuring Access Control for Outgoing Calls " in the chapter "Configuring Legacy DDR Hubs."
DDR and dialer commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference* , Release 12.2.

Related Topic	Document Title
PPPoE Stage Protocols	*Cisco IOS Wide-Area Networking Configuration Guide* , Release 12.2. See the section "PPPoE Stage Protocols" in the chapter "Configuring Broadband Access: PPP and Routed Bridge Encapsulation."
PPPoE configuration commands: complete command syntax, command mode, defaults, usage guidelines, and example	*Cisco IOS Wide-Area Networking Command Reference* , Release 12.2. See the chapter "Broadband Access: PPP and Routed Bridge Encapsulation Commands."

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for PPPoE Client DDR Idle-Timer

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 Client DDR Idle-Timer

Feature Name	Releases	Feature Information
PPPoE Client DDR Idle-Timer	12.2(13)T	The PPPoE Client DDR Idle-Timer feature supports the dial-on-demand routing (DDR) interesting traffic control list functionality of the dialer interface with a PPP over Ethernet (PPPoE) client, but also keeps original functionality (PPPoE connection up and always on after configuration) for those PPPoE clients that require it. This feature is supported on Cisco 806, Cisco 827, Cisco SOHO 70 series routers. The following commands were introduced or modified: **pppoe-client dial-pool-number**.

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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for 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 201 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 introduced in Cisco IOS Release 12.3(4)T 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 202 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.

RADIUS Subscriber Profile Entry for the LAC

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"
```

RADIUS VPDN Group User Profile Entry for the LNS

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
```

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.

	Command or Action	Purpose
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 204 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 204

What to Do Next

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *vpdn-group-name* **Example:** `Router(config)# vpdn-group Group-A`	Creates a VPDN group and enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from an LAC and creates an accept-dialin VPDN subgroup.
Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP tunneling protocol.
Step 6	**virtual-template** *template-number* **Example:** `Router(config-vpdn-req-in)# virtual-template 2`	Specifies which virtual template will be used to clone virtual access interfaces.
Step 7	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits to VPDN group configuration mode.

	Command or Action	Purpose
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 Monitoring PPPoE Relay, page 206 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
```

Step 4 **clear pppoe relay context**

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

Example:

```
Router# clear pppoe relay context
```

- Troubleshooting Tips, page 207

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, page 208
- Basic LNS Configured for PPPoE Relay Example, page 208
- Tunnel Switch (or Multihop Node) Configured to Respond to PAD Messages Example, page 210
- Tunnel Switch Configured to Relay PAD Messages Example, page 211

- RADIUS Subscriber Profile Entry for the LAC Example, page 211
- RADIUS VPDN Group User Profile Entry for the LNS Example, page 211

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 Sample1.net
.
.
.
vpdn-group Sample2.net
! Configure L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from host Host1
 relay pppoe bba-group group-1
.
.
.
vpdn-group Sample1.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 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 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	Configuring Virtual Private Networks chapter in the Virtual Templates, Profiles, and Networks section of the *Cisco IOS Dial Technologies Configuration Guide*
VPDN tunnel commands	*Cisco IOS Dial Technologies Command Reference*
Tunnel switching	L2TP Tunnel Switching feature module
PPPoE broadband groups	Refer to the chapters in the "Broadband Access" part of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.3.
PPPoE broadband commands	*Cisco IOS Wide-Area Networking Command Reference*, Release 12.3
Broadband access aggregation concepts	Refer to the Understanding Broadband Access Aggregation module.
Tasks for preparing for broadband access aggregation	Refer to the Preparing for Broadband Access Aggregation module.

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
RFC 2516	"Method for Transmitting PPP Over Ethernet (PPPoE)"
RFC 3817	L2TP Active Discovery Relay for PPPoE Network Working Group Internet-Draft, *L2TP Active Discovery Relay for PPPoE* , which can be seen at http://tools.ietf.org/html/draft-dasilva-l2tp-relaysvc-06

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	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 11 Feature Information for Enabling PPPoE Relay Discovery and Service Selection Functionality

Feature Name	Releases	Feature Configuration Information
PPPoE Relay	12.3(4)T	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).

Establishing PPPoE Session Limits per NAS Port

The PPPoE Session Limits per NAS Port feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions on a specific permanent virtual circuit (PVC) or VLAN configured on an L2TP access concentrator (LAC). The network access server (NAS) port is either an ATM PVC or a configured VLAN ID. PPPoE per-NAS-port session limits are maintained in a RADIUS server customer profile database and are downloaded during Subscriber Service Switch (SSS) preauthorization.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Establishing PPPoE Session Limits per NAS Port

You must understand the concepts described in the "Preparing for Broadband Access Aggregation" module.

Both the LAC and the L2TP Network Server (LNS) must be running a Cisco IOS image that supports the PPPoE Session Limit Per NAS Port feature.

Protocol support for broadband access aggregation must be established using the procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module.

Restrictions for Establishing PPPoE Session Limits per NAS Port

- Do not configure the PPPoE per-NAS-port session limit to zero.
- PPPoE Session Limit per NAS Port does not support TACACS+.
- PPPoE Session Limit per NAS Port applies only to PVCs and VLANs.

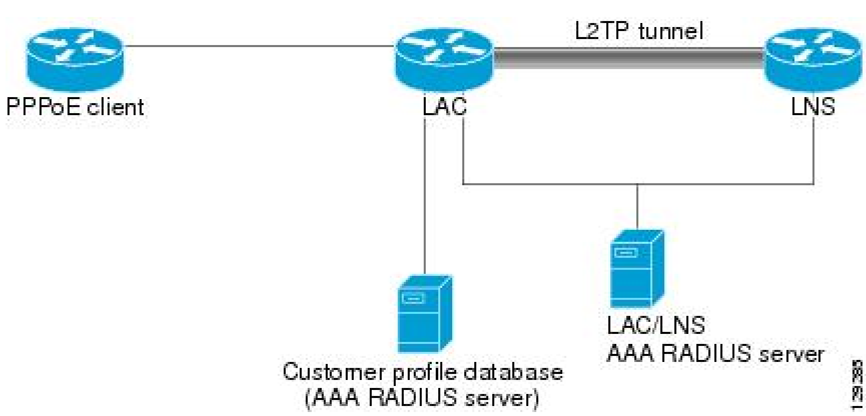
Information About Establishing PPPoE Session Limits per NAS Port

How PPPoE per-NAS-Port Session Limits Work

The PPPoE Session Limits Per NAS Port feature limits the number of PPPoE sessions on a specific PVC or VLAN configured on an LAC. The NAS port is either an ATM PVC or a configured VLAN ID.

The PPPoE per-NAS-port session limit is maintained in a RADIUS server customer profile database. This customer profile database is connected to an LAC and is separate from the RADIUS server that the LAC and LNS use for the authentication and authorization of incoming users. See below for a sample network topology. When the customer profile database receives a preauthorization request from the LAC, it sends the PPPoE per-NAS-port session limit to the LAC.

The LAC sends a preauthorization request to the customer profile database when the LAC is configured for SSS preauthorization. When the LAC receives the PPPoE per-NAS-port session limit from the customer profile database, the LAC compares the PPPoE per-NAS-port session limit with the number of sessions currently on the NAS port. The LAC then decides whether to accept or reject the current call, depending upon the configured PPPoE per NAS port-session-limit and the number of calls currently on the NAS port.
PPPoE Session Limit per NAS Port Sample Topology



The customer profile database consists of a user profile for each user that is connected to the LAC. Each user profile contains the NAS-IP-Address (attribute 4) and the NAS-Port-ID (attribute 5.) When the LAC is configured for SSS preauthorization, it queries the customer profile database using the username. When a match is found in the customer profile database, the customer profile database sends the PPPoE per-NAS-port session limit in the user profile. The PPPoE per-NAS-port session limit is defined in the username as a Cisco attribute-value (AV) pair.

Relationship Between the Per-NAS-Port Session Limit and Other Types of Session Limits

You can configure types of session limits other than per-NAS-sort sessions on the LAC, including session limit per VC, per VLAN, per MAC, and a global session limit for the LAC. When PPPoE session limits for a NAS port are enabled (that is, when you have enabled SSS preauthorization on the LAC), local configurations for session limits per VC and per VLAN are overwritten by the PPPoE per-NAS-port session limit downloaded from the customer profile database. Configured session limits per VC and per VLAN serve as backups in case of a download failure of the PPPoE per-NAS-port session limit. Global session limits and per-MAC session limits, if configured on the router, will take effect as other means of limiting PPPoE sessions.

Benefits of PPPoE Session Limits per NAS Port

PPPoE session limits per NAS port provides flexibility and simplifies router configuration by allowing you to download the per-VC and per-VLAN session limits from a RADIUS server in addition to being able to configure them on the router.

How to Establish PPPoE Session Limits per NAS Port

Enabling Subscriber Service Switch Preauthorization

When SSS 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 SSS preauthorization:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber access pppoe pre-authorize nas-port-id** [*aaa-method-list*]
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 access pppoe pre-authorize nas-port-id** [*aaa-method-list*] **Example:** `Router(config)# subscriber access pppoe pre-authorize nas-port-id mlist-llid` **Example:**	Enables SSS preauthorization. • *aaa-method-list* --Name of an authentication, authorization and accounting (AAA) list configured on the LAC. **Note** During SSS preauthorization, per-NAS-port session limits are downloaded to the LAC.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the RADIUS User Profile for PPPoE Session Limits per NAS Port

Perform the following steps to enable per-NAS-port PPPoE session limits in a RADIUS user profile for the customer profile database. Refer to the Cisco IOS Security Configuration Guide for information about creating a RADIUS user profile.

SUMMARY STEPS

1. User-Name = nas-port:ip-address:slot/subslot/port/vpi.vci
2. User-Name = nas-port:ip-address:slot/subslot/port/vlan-id
3. User-Name = nas-port:ip-address:slot/subslot/port/vlan-id
4. Password = "cisco"
5. cisco-avpair = "pppoe:session-limit-session-limit-per-NAS-port"

DETAILED STEPS

	Command or Action	Purpose
Step 1	User-Name = nas-port:ip-address:slot/subslot/port/vpi.vci	Configures the NAS port username for a PPPoE over ATM NAS port user. • *ip-address* --IP address of the LAC interface that connects to the customer profile database. • *slot* /*subslot*/*port*--ATM interface. • *vpi.vci* --Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.
Step 2	User-Name = nas-port:ip-address:slot/subslot/port/vlan-id	Configures the NAS port username for a PPPoE over ATM NAS port user. • *ip-address* --IP address of the LAC interface that connects to the customer profile database. • *slot* /*subslot*/*port*--ATM interface. • *vpi.vci* --Virtual path identifier (VPI) and virtual channel identifier (VCI) values for the PVC.
Step 3	User-Name = nas-port:ip-address:slot/subslot/port/vlan-id **Example:**	Configures the NAS port username for a PPPoE over VLAN NAS port user. • *ip-address* --IP address of the LAC interface that connects to the customer profile database. • *slot* /*subslot*/*port*--ATM interface. • *vlan-id* --VLAN identifier.
Step 4	Password = "cisco" **Example:**	Sets the fixed password.
Step 5	cisco-avpair = "pppoe:session-limit-session-limit-per-NAS-port"	Adds the PPPoE session limit per NAS port cisco AVpair to the user profile. • *session-limit-per-NAS-port* --per-NAS-port PPPoE session limit.

Verifying PPPoE Session Limit per NAS Port

Perform this task to verify per-NAS-port session limit performance.

SUMMARY STEPS

1. **enable**
2. **debug aaa authorization**
3. **debug radius** [**brief** | **hex**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information about AAA authorization.
Step 3	**debug radius** [**brief** | **hex**] **Example:** `Router(config)# debug radius`	Displays information about RADIUS.

Configuration Examples for Establishing PPPoE Session Limits per NAS Port

Configuring the LAC for per-NAS-Port Session Limits for PPPoE over ATM Example

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-mac**, **pppoe limit per-vc**, and **pppoe limit per-vlan** commands are replaced by the **sessions per-mac limit**, **sessions per-vc limit**, and **sessions per-vlan limit** commands, respectively, in bba-group configuration mode. See the **sessions per-mac limit**, **sessions per-vc limit**, and **sessions per-vlan limit** commands for more information.

The following example shows how to configure per-NAS-port session limits for PPPoE over ATM on the LAC:

```
!
username lac password 0 lab
username lns password 0 lab
aaa new-model
!
```

```
aaa authentication ppp default group radius local
aaa authentication ppp mlist-nasport group radius
aaa authorization network mlist-nasport group radius
aaa session-id common
ip subnet-zero
!
no ip domain lookup
ip host abrick 209.165.200.225
!
ip cef
subscriber access pppoe pre-authorize nas-port-id mlist-nasport
vpdn enable
!
vpdn-group l2tp-initiator
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.2
 local name lac
!
vpdn-group pppoe-terminate
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 10
 pppoe limit per-vc 10
 pppoe limit per-vlan 10
!
vc-class atm pppoe
  protocol pppoe
  ubr 155000
  encapsulation aal5snap
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 class-int pppoe
 pvc 1/100
  encapsulation aal5snap
 !
!
interface FastEthernet4/0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 duplex full
!
interface FastEthernet6/0
 ip address 10.165.200.225 255.255.255.0
 no ip mroute-cache
 duplex full
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap mlist-nasport
!
ip default-gateway 10.3.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.0.1
!
!
ip radius source-interface FastEthernet6/0
!
radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server authorization permit missing Service-Type
!
```

Configuring the LAC for per-NAS-Port Session Limits for PPPoE over VLAN Example

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-mac**, **pppoe limit per-vc**, and **pppoe limit per-vlan** commands are replaced by the **sessions per-mac limit**, **sessions per-vc limit**, and **sessions per-vlan limit** commands, respectively, in bba-group configuration mode. See the **sessions per-mac limit**, **sessions per-vc limit**, and **sessions per-vlan limit** commands for more information.

The following example shows how to configure per-NAS-port session limits for PPPoE over VLAN on the LAC:

```
!
username lac password 0 lab
username lns password 0 lab
aaa new-model
!
!
aaa authentication ppp default group radius local
aaa authentication ppp mlist-nasport group radius
aaa authorization network mlist-nasport group radius
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip host abrick 192.0.2.0
!
ip cef
subscriber access pppoe pre-authorize nas-port-id mlist-nasport
vpdn enable
!
vpdn-group l2tp_initiator
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.2
 local name lac
!
vpdn-group pppoe-terminate
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 10
 pppoe limit per-vc 10
 pppoe limit per-vlan 10
!
vc-class atm pppoe
  protocol pppoe
  ubr 155000
  encapsulation aal5snap
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet4/0
 ip address 10.1.1.1 255.255.255.0
 no ip mroute-cache
 duplex full
!
interface FastEthernet6/0
 ip address 224.0.0.0 255.255.255.0
```

```
 no ip mroute-cache
 duplex full
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap mlist-nasport
!
ip default-gateway 224.0.0.0
ip classless
ip route 0.0.0.0 0.0.0.0 224.0.0.0
!
!
ip radius source-interface FastEthernet6/0
!
!
!
radius-server host 10.1.1.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server authorization permit missing Service-Type
!
```

Configuring the User Profile for PPPoE Session Limits per NAS Port Example

The following example shows how to configure the user profile for PPPoE session limits per NAS port. In this example, the user has a PVC with a VPI of 1 and a VCI of 100 on ATM interface 4/0/0 of the LAC with an IP address of 10.10.10.10:

```
Username=nas_port:10.10.10.10:4/0/0/1.100
Password = "password1"
cisco-avpair= "pppoe:session-limit=<session limit per NAS-port>"
```

Where to Go Next

- If you want to use service tags to enable a PPPoE server to offer PPPoE clients a selection of services 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 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 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
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	"Wide-Area Networking Commands" chapter in the *Cisco IOS Wide-Area Networking Command Reference*
Broadband access aggregation concepts	*"* Understanding Broadband Access Aggregation*"*
Task for preparing for broadband access aggregation	"Preparing for Broadband Access Aggregation"
Broadband access aggregation support	"Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions"

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2516	*A Method for Transmitting PPP over Ethernet (PPPoE)*
RFC 2684	*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 Establishing PPPoE Session Limits per NAS Port

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 PPoE Session Limit per NAS Port.

Feature Name	Releases	Feature Information
PPPoE Session Limit per NAS Port	12.2(31)SRC 12.2(15)B 12.3(4)T	The PPPoE Session Limit per NAS Port feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions on a specific permanent virtual circuit (PVC) or VLAN configured on an L2TP access concentrator (LAC). In Cisco IOS Release 12.2(15)B, this feature was introduced. In Cisco IOS Release 12.3(4)T, this feature was integrated into the T train.

Offering PPPoE Clients a Selection of Services During Call Setup

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. The customer chooses 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 customers according to the service chosen.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Offering PPPoE Clients a Selection of Services During Call Setup

- The PPPoE Service Selection feature requires that PPPoE 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 are going to use PPPoE service selection to offer tunneling services, the procedures in this document assume that you already have tunneling configured and working.

Information About Offering PPPoE Clients a Selection of Services During Call Setup

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 as it would 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 will 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 will advertise 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 will be 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 will be advertised to the client.

The Cisco RADIUS vendor-specific attribute (VSA) "service-name" will be 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 will be 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 will be applied to the permanent virtual circuit (PVC) on which the PPPoE call is coming in.

The Configuring the Subscriber Profile for PPPoE Service Selection, page 230 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 customers and to charge customers 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 customers 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 13 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 will be 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 will be applied to the ATM PVC on which a PPPoE session is being established.

Attributes Used 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.

Prerequisites

The default AAA authorization method list determines where the policy manager looks for the subscriber profile. When the subscriber profile is configured remotely, the **aaa authorization network default group radius**command must be included in the AAA configuration so the policy manager knows to look for the subscriber policy on a AAA server. These attributes are defined while configuring the RADIUS server. Refer to the RADIUS server documentation for information about how to perform this configuration.

Table 14 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 will be listed in this subscriber profile.

How to Offer PPPoE Clients a Selection of Services During Call Setup

Configuring the Subscriber Profile for PPPoE Service Selection

The subscriber profile contains the list of services that will be 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. **subscriber profile** *profile-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**

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-name`	Enters SSS profile configuration mode. Defines the Subscriber Service Switch policy for searches of a subscriber profile database.
Step 4	**pppoe service** *service-name* **Example:** `Router(config-sss-profile)# 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-sss-profile)# end`	(Optional) Terminates the configuration session and returns to privileged EXEC 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. **service profile** *subscriber-profile-name* [**refresh** *minutes*]
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 group1`	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	**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.

	Command or Action	Purpose
Step 5	**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 will advertise 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 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 6	**end** **Example:** `Router(config-bba-group)# end`	(Optional) Returns to privileged EXEC mode.

- Troubleshooting Tips, page 233
- What to Do Next, page 233

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 (Ethernet interface, 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" module.

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** *interface-number*[**.** *subinterface-number* **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** *interface-number*[**.** *subinterface-number* **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 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 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 10.0.0.1:1824, 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  "4085554206"
00:02:50: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:02:50: RADIUS:  Calling-Station-Id  [31]  12  "4085554206"
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  "00000002"
00:02:50: RADIUS:  Delay-Time          [41]  6   0
00:02:51: RADIUS: Received from id 0 1.7.157.1:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
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 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
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  "4085554206"
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 1 1.7.157.1:1823, 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 4085274206, 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 2 1.7.157.1:1824, 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  "4085274206"
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 2 1.7.157.1:1824, 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  "00000002"
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 6 10.0.0.1:1824, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
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:23 id 8 10.0.0.0:1823, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 8 1.7.157.1:1823, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:23 id 9 10.0.0.1:1824, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 9 1.7.157.1:1824, 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:23 id 10 10.0.0.1:1824, 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 0000000921156833323322D67772D69643D353330305F34332E
17:26:52:         Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D38463341333136333204234393830303046
20302033424537314238
17:26:52:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:26:52:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:26:52:         Attribute 26 56
00000009193268333232D73657475702D74696D653D2A30393A32363A35322E38383020505354205361742 04A
616E20312032303030
17:26:52:         Attribute 26 48
00000009182A683332332D636F6E662D69643D38463341333136333204234393830303046203020334245373142
38
17:26:52:         Attribute 44 10 3030303030303035
17:26:52:         Attribute 41 6 00000000
17:26:52: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
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
00000009182A683332332D636F6E662D69643D38463341333136333204234393830303046203020334245373142
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 1.7.157.1:1823, Access-Accept, len 115
17:27:01:         Attribute 6 6 00000001
17:27:01:         Attribute 26 29 00000009651768333232D6372656469742D616D6F756E743D3435
17:27:01:         Attribute 26 27 00000009661568333232D6372656469742D74696D653D3333
17:27:01:         Attribute 26 26 00000009671468333232D72657475726E2D636F64653D30
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 4085554206, 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 1.7.157.1:1824, 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 0000000921156833323322D67772D69643D353330305F34332E
17:27:09:         Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D38463341333136333204234393830303046
20302033424537314238
17:27:09:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:27:09:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:27:09:         Attribute 26 56
00000009193268333232D73657475702D74696D653D2A30393A32363A35322E38383020505354205361742 04A
616E20312032303030
17:27:09:         Attribute 26 58
```

```
000000091C34683332332D636F6E6E6563742D74696D653D2A30393A32363A35322E393037205053542053617420A616E20312032303030
17:27:09:        Attribute 26 61
000000091D37683332332D646973636F6E6E6563742D74696D653D2A30393A32373A31302E313337205053542053617420A616E20312032303030
17:27:09:        Attribute 26 32
000000091E1A683332332D646973636F6E6E6563742D63617573653D3130
17:27:09:        Attribute 26 28 000000091F16683332332D766F6963652D7175616C6974793D30
17:27:09:        Attribute 26 48
00000009182A683332332D636F6E662D69643D38463341333136332042343938303030462030203342453731 4238
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 0000000901187375627363726962652723D526567756C61724C696E65
17:27:09:        Attribute 26 35
00000009011D683332332D6976722D6F75743D5461726966663A556E6B6E6F776E
17:27:09:        Attribute 26 22 0000000901107072652D62797465732D696E3D30
17:27:09:        Attribute 26 23 0000000901117072652D62797465732D6F75743D30
17:27:09:        Attribute 26 21 00000009010F7072652D70616B732D696E3D30
17:27:09:        Attribute 26 22 0000000901107072652D70616B732D6F75743D30
17:27:09:        Attribute 26 22 0000000901106E61732D72782D73706565643D30
17:27:09:        Attribute 26 22 0000000901106E61732D74782D73706565643D30
17:27:09:        Attribute 41 6 00000000
17:27:09: RADIUS: Received from id 12 10.0.0.1:1824, Accounting-response, len 20
```

Configuration Examples for PPPoE Service Selection

PPPoE Service Selection with ATM QoS and Tunneling Services Example

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 will be 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
subscriber profile  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  5
 service profile listA
!
! Attach the PPPoE profile to a PVC
interface atm1/0.1
 pvc 2/200
  protocol PPPoE group group-A
!
```

PPPoE Service Selection with Tunneling Services Example

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 atm1/0.1
 pvc 2/200
  protocol PPPoE group pppoe-group-A
!
interface atm1/0.2
 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 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

The following sections provide references related to PPPoE service selection.

Related Documents

Related Topic	Document Title
RADIUS configuration	*"Configuring RADIUS" chapter of the Cisco IOS Security Configuration Guide, Release 12.3*
RADIUS attributes	"RADIUS Attributes" appendix to the *Cisco IOS Security Configuration Guide, Release 12.3*
Tunneling configuration	*"Configuring Virtual Private Networks" chapter of the Cisco IOS Dial Technologies Configuration Guide, Release 12.3*

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Task for preparing for broadband access aggregation.	Preparing for Broadband Access Aggregation
Broadband access commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	"Wide-Area Networking Commands" chapter in the *Cisco IOS Wide-Area Networking Command Reference*, Release 12.3
Configuring 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. 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 IOS 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/techsupport

Feature Information for Offering PPPoE Clients a Selection of Services During Call Setup

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

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

Table 15 Feature Information for Offering PPPoE Clients a Selection of Services During Call Setup

Feature Name	Releases	Feature Configuration Information
PPPoE Service Selection	12.3(4)T 12.2(33)SRC	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. The customer chooses one of the services offered, and the service is provided when the PPPoE session becomes active.

Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

The Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs feature provides the functionality of bridged ATM interface support to ATM switched virtual circuits (SVCs). Unlike permanent virtual circuits (PVCs), SVCs must be triggered by ongoing traffic and can be brought down when idle for some time. The SVCs are triggered, if down, and the traffic is passed on to the SVCs belonging to bridged ATM interface.

ATM routed bridge encapsulation (RBE) is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

- When ATM SVCs are used, support for a form of bridging, such as integrated routing and bridging, is required.
- Before configuring connectivity from a remote bridged Ethernet network to a routed network using ATM routed bridge encapsulation, you must understand the concepts in the Understanding Broadband Access Aggregation module.

Restrictions for Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

- Unlike PVCs, SVCs must be triggered by ongoing traffic and might be brought down after they have been idle for some time. The Bridged 1483 Encapsulated Traffic over ATM SVCs feature allows for the SVC to be triggered if down, and to pass the traffic on to the SVCs belonging to the bridged ATM interface.
- ATM RBE does not support MAC-layer access lists; only IP access lists are supported.

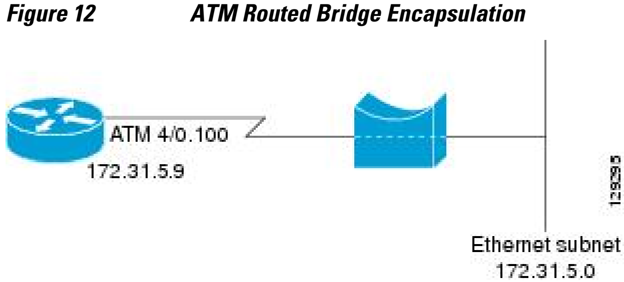
Information About Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

Overview on Bridged 1483 Encapsulated Traffic over ATM SVCs

ATM RBE is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

The figure below shows an ATM subinterface on a headend router that is configured to function in ATM routed-bridge encapsulation mode. This configuration is useful when a remote bridged Ethernet network device needs connectivity to a routed network via a device bridging from an Ethernet LAN to an ATM RFC 1483 bridged encapsulation.

Figure 12 ATM Routed Bridge Encapsulation



Because PVCs are statically configured along the entire path between the end systems, it would not be suitable to route bridged encapsulated traffic over them when the user wants to configure the virtual circuits (VCs) dynamically and tear down the VCs when there is no traffic.

ATM RBE Subinterface Grouping by PVC Range

You can configure ATM routed bridge encapsulation using an ATM PVC range rather than individual PVCs. When you configure a PVC range for routed bridge encapsulation, a point-to-point subinterface is created for each PVC in the range. The number of PVCs in a range can be calculated using the following formula:

number of PVCs = (end-vpi - start-vpi + 1) x (end-vci - start-vci +1)

Subinterface numbering begins with the subinterface on which the PVC range is configured and increases sequentially through the range.

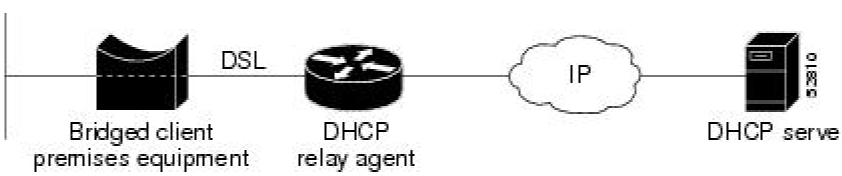
Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

DHCP Option 82 Support for RBE

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

The DHCP Option 82 Support for RBE feature provides support for the DHCP relay agent information option when ATM RBE is used. The figure below shows a typical network topology in which ATM RBE and DHCP are used. The aggregation router that is using ATM RBE is also serving as the DHCP relay agent.

Figure 13 Network Topology Using ATM RBE and DHCP



This feature communicates information to the DHCP server using a suboption of the DHCP relay agent information option called agent remote ID. The information sent in the agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

The figure below shows the format of the agent remote ID suboption.

Figure 14 Format of the Agent Remote ID Suboption

1 12 bytes

Port type (byte 1)	Version (byte 2)	Reserved (bytes 3-4)	NAS IP address (bytes 5-8)	NAS port (bytes 9-12)

53811

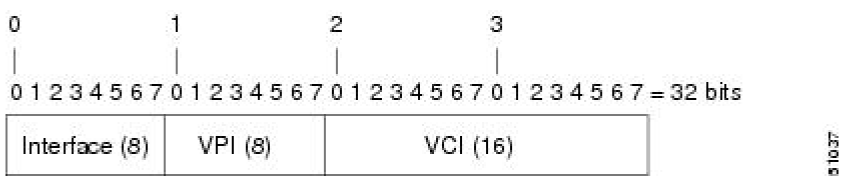
The table below describes the agent remote ID suboption fields displayed in the figure above.

Table 16 Agent Remote ID Suboption Field Descriptions

Field	Description
Port Type	Port type. The value 0x01 indicates RBE. (1 byte)
Version	Option 82 version. The value 0x01 specifies the RBE version of Option 82 (1 byte).
Reserved	RBE reserved (2 bytes).
NAS IP Address	One of the interfaces on the DHCP relay agent. The **rbe nasip** command can be used to specify which IP address will be used. (4 bytes)
NAS Port	RBE-enabled virtual circuit on which the DHCP request has come in. See the figure below for the format of this field. (4 bytes)

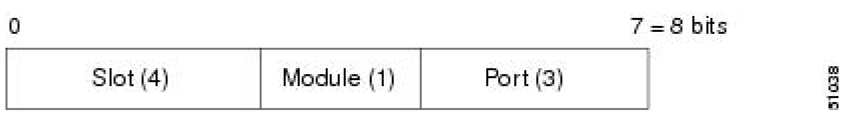
The figure below shows the format of the network access server (NAS) port field in the agent remote ID suboption.

Figure 15 Format of the NAS Port Field



The figure below shows the format of the interface field. If there is no module, the value of the module bit is 0.

Figure 16 Format of the Interface Field



DHCP Lease Limit per ATM RBE Unnumbered Interface

The DHCP lease limit per ATM RBE Unnumbered Interface feature is enabled on a Cisco IOS DHCP relay agent connected to clients through unnumbered interfaces. The relay agent keeps information about the DHCP leases offered to the clients per subinterface. When a DHCPACK message is forwarded to the client, the relay agent increments the number of leases offered to clients on that subinterface. If a new DHCP client tries to obtain an IP address and the number of leases has already reached the configured lease limit, DHCP messages from the client will be dropped and will not be forwarded to the DHCP server.

If this feature is enabled on the Cisco IOS DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

ATM Routed Bridge Encapsulation Support with SSO and ISSU

Cisco IOS High Availability (HA) functionality for broadband protocols and applications allows for stateful switchover (SSO) and In-Service Software Upgrade (ISSU) that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to synchronize the subscriber sessions on the standby processor of a redundant processor system. Use the **show ccm clients** command to display information about the CCM clients. Use the **show ccm sessions** command to display information about CCM sessions on active and standby processors. Use the **show subscriber policy** command to display information about subscriber redundancy policies.

In Cisco IOS Release 15.1(1)S and later releases, all ATM RBE features are supported with SSO and ISSU.

Benefits of Providing Connectivity Using ATM Routed Bridge Encapsulation

Bridged IP packets received on an ATM interface configured in routed-bridge mode are routed via the IP header. Such interfaces take advantage of the characteristics of a stub LAN topology commonly used for digital subscriber line (DSL) access and offer increased performance and flexibility over integrated routing and bridging (IRB).

Another benefit of ATM RBE is that it reduces the security risk associated with normal bridging or IRB by reducing the size of the nonsecured network. By using a single VC allocated to a subnet (which could be as small as a single IP address), ATM RBE uses an IP address in the subnet to limit the "trust environment" to the premises of a single customer.

ATM RBE supports Cisco Express Forwarding (CEF), fast switching, and process switching.

The DHCP Option 82 Support for RBE feature enables those service providers to use DHCP to assign IP addresses and DHCP option 82 to implement security and IP address assignment policies.

The DHCP Lease Limit per ATM RBE Unnumbered Interface feature allows an Internet service provider (ISP) to globally limit the number of leases available to clients per household or connection.

How to Configure ATM Routed Bridge Encapsulation over PVCs

Configuring ATM Routed Bridge Encapsulation Using PVCs

Perform the following task to configure ATM RBE using PVCs. Only the specified network layer (IP) is routed. Any remaining protocols can be passed on to bridging or other protocols. In this manner, ATM RBE can be used to route IP, while other protocols (such as IPX) are bridged normally.

or

show ip cache verbose

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* **/ 0 .** *subinterface-number* **point-to-point** **Example:** `Router(config)# interface atm 5/0.5 point-to-point`	Specifies an ATM point-to-point subinterface and enters subinterface mode.

	Command or Action	Purpose

Step 4	Do one of the following:
	• **pvc** *vpi* /*vci*
	•
	• **range** [*range-name*] **pvc** *start-vpi* / *start-vci end-vpi* / *end-vci*
	
	Example:
	`Router(config-subif)# pvc 0/32`
	
	Example:
	`Router(config-subif)# range range1 pvc 1/200 1/299`
		Configures a PVC to carry the routed bridge traffic and enters ATM VC class configuration mode.
		Configures a range of PVCs to carry the routed bridge traffic and enters ATM PVC range configuration mode.

Step 5	**exit** **Example:** `Router(config-if-atm-vc)# exit`	Exits to subinterface configuration mode.
Step 6	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-subif)# ip address 209.165.200.224 255.255.255.0`	Provides an IP address on the same subnetwork as the remote network.
Step 7	**end** **Example:** `Router(config-subif)# end`	Exits to privileged EXEC mode.

Step 8	Do one of the following:
	• **show arp**
	• or
	• **show ip cache verbose**
	
	Example:
	`Router# show arp`
	
	Example:
	`Router# show ip cache verbose`
		(Optional) Displays ATM RBE configuration information.

Examples

To confirm that ATM RBE is enabled, use the **show arp** command and the **show ip cache verbose** command in privileged EXEC mode:

```
Router# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet     209.165.201.51          6   0001.c9f2.a81d  ARPA   Ethernet3/1
Internet     209.165.201.49          -   0060.0939.bb55  ARPA   Ethernet3/1
Internet 209.165.202.128         30   0010.0ba6.2020  ARPA   Ethernet3/0
Internet 209.165.201.52           6   00e0.1e8d.3f90  ARPA   ATM1/0.4
Internet 209.165.201.53           5   0007.144f.5d20  ARPA   ATM1/0.2
Internet 209.165.202.129          -   0060.0939.bb54  ARPA   Ethernet3/0
Internet 209.165.201.125         30   00b0.c2e9.bc55  ARPA   Ethernet3/1#
Router# show ip cache verbose
IP routing cache 3 entries, 572 bytes
   9 adds, 6 invalidates, 0 refcounts
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last second, 0 in last 3 seconds
Last full cache invalidation occurred 00:30:34 ago
Prefix/Length       Age       Interface     Next Hop
209.165.201.51/32-24 00:30:10  Ethernet3/1 10.1.0.51 14  0001C9F2A81D00600939 BB550800
209.165.202.129/32-24 00:00:04 ATM1/0.2     10.8.100.50 28
00010000AAAA030080C2000700000007144F5D2000600939 BB1C0800
209.165.201.125/32-24 00:06:09 ATM1/0.4     10.8.101.35 28
00020000AAAA030080C20007000000E01E8D3F9000600939 BB1C0800
```

Configuring DHCP Option 82 for RBE

Perform this task to configure the DHCP Option 82 Support for RBE feature.

DHCP option 82 support must be configured on the DHCP relay agent using the **ip dhcp relay information option** command before you can use the DHCP Option 82 Support for RBE feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **rbe nasip** *source-interface*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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	**ip dhcp relay information option** **Example:** `Router(config)# ip dhcp relay information option`	Enables the DHCP option 82 support on relay agent. • Enabling the DHCP option 82 support allows the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.
Step 4	**rbe nasip** *source-interface* **Example:** `Router(config)# rbe nasip loopback0`	Specifies the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the Agent Remote ID suboption.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged configuration mode.

Configuring the DHCP Lease Limit

Perform this task to limit the number of DHCP leases allowed on ATM RBE unnumbered or serial unnumbered interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease per interface** *lease-limit*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp limit lease per interface** *lease-limit* **Example:** `Router(config)# ip dhcp limit lease per interface 2`	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting the DHCP Lease Limit

Perform this task to troubleshoot the DHCP lease limit.

SUMMARY STEPS

1. **enable**
2. **debug ip dhcp server packet**
3. **debug ip dhcp server events**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**debug ip dhcp server packet** **Example:** `Router# debug ip dhcp server packet`	(Optional) Decodes DHCP receptions and transmissions.
Step 3	**debug ip dhcp server events** **Example:** `Router(config)# debug ip dhcp server events`	(Optional) Displays server events.

Configuration Examples for Providing Connectivity Using ATM Routed Bridge Encapsulation

The following examples show various ways to provide connectivity from a remote bridged network to a routed network using ATM RBE.

- Example Configuring ATM RBE on PVCs, page 255
- Example Configuring ATM RBE on an Unnumbered Interface, page 255
- Example Concurrent Bridging and ATM RBE, page 256
- Example DHCP Option 82 for RBE Configuration, page 256
- Example DHCP Lease Limit, page 257

Example Configuring ATM RBE on PVCs

The following example shows a typical ATM routed bridge encapsulation configuration:

```
enable
 configure terminal
 interface atm 4/0.100 point-to-point
  ip address 209.165.200.225 255.255.255.224
   pvc 0/32
    end
```

Example Configuring ATM RBE on an Unnumbered Interface

The following example uses a static route to point to an unnumbered interface:

```
enable
 configure terminal
 interface loopback 0
 ip address 209.165.200.226 255.255.255.224
 interface atm 4/0.100 point-to-point
  ip unnumbered loopback 0
  pvc 0/32
   atm route-bridge ip
   exit
```

```
  ip route 209.165.200.228 255.255.255.224 atm 4/0.100
  end
```

Example Concurrent Bridging and ATM RBE

The following example shows concurrent use of ATM RBE with normal bridging. IP datagrams are route-bridged, and other protocols (such as IPX or AppleTalk) are bridged.

```
bridge 1 protocol ieee
interface atm 4/0.100 point-to-point
 ip address 209.165.200.225 255.255.255.224
 pvc 0/32
 bridge-group 1
 atm route-bridge ip
```

Example DHCP Option 82 for RBE Configuration

In the following example, DHCP option 82 support is enabled on the DHCP relay agent using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server.

```
ip dhcp-server 209.165.200.225
!
ip dhcp relay information option
!
interface Loopback0
 ip address 209.165.201.0 255.255.255.248
!
interface atm 4/0
 no ip address
!
interface atm 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 209.165.201.3
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
!
interface Ethernet5/1
 ip address 209.165.201.4 255.255.255.248
!
router eigrp 100
 network 209.165.201.0
 network 209.165.200.0
!
rbe nasip Loopback0
```

For the configuration example, the value (in hexadecimal) of the agent remote ID suboption would be 010100000B01018140580320. The table below shows the value of each field within the agent remote ID suboption.

Table 17 Agent Remote ID Suboption Field Values

Agent Remote ID Suboption Field	Value
Port Type	0x01
Version	0x01
Reserved	undefined

Agent Remote ID Suboption Field	Value
NAS IP Address	0x0B010181 (hexadecimal value of 11.1.1.129)
NAS Port • Interface (slot/module/port) • VPI • VCI	• 0x40 (The slot/module/port values are 01 00/0/000.) • 0x58 (hexadecimal value of 88) • 0x320 (hexadecimal value of 800)

Example DHCP Lease Limit

In the following example, if more than three clients try to obtain an IP address from interface ATM4/0.1, the DHCPDISCOVER packets will not be forwarded to the DHCP server. If the DHCP server resides on the same router, DHCP will not reply to more than three clients.

```
ip dhcp limit lease per interface 3
!
interface loopback0
 ip address 209.165.201.3 255.255.255.248
!
interface atm 4/0.1
 no ip address
!
interface atm 4/0.1 point-to-point
 ip helper-address 172.16.1.2
 ip unnumbered loopback0
 atm route-bridged ip
  pvc 88/800
  encapsulation aal5snap
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Broadband Access Aggregation and DSL commands	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Preparing for broadband access aggregation task	Preparing for Broadband Access Aggregation
DHCP commands	*Cisco IOS IP Addressing Services Command Reference*
DHCP configuration tasks	"Configuring the Cisco IOS DHCP Server" module in the *Cisco IOS IP Addressing Services Configuration Guide*

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

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

Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation

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

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

Table 18 Feature Information for Providing Connectivity Using ATM Routed Bridge Encapsulation

Feature Name	Releases	Feature Information
RBE-SSO	15.1(1)S	ATM RBE features are supported with SSO.
RBE-ISSU	15.1(1)S	ATM RBE features are supported with ISSU.
Bridged 1483 Encapsulated Traffic over ATM SVCs	12.4(15)T 12.2(33)SRE	The Bridged 1483 Encapsulated Traffic over ATM SVCs feature provides support for bridged 1483 encapsulated packets to trigger ATM SVC and also support for sending this traffic on triggered ATM SVCs.
DHCP Option 82 Support for Routed Bridge Encapsulation	15.1(1)S 12.2(2)T	This feature provides support for the DHCP relay agent information option when ATM RBE is used. The following command was introduced:**rbe nasip**
DHCP Lease Limit per ATM RBE Unnumbered Interface	12.3(2)T	This feature limits the number of DHCP leases per subinterface offered to DHCP clients connected from an ATM RBE unnumbered interface or serial unnumbered interface of the DHCP server or DHCP relay agent. The following command was introduced:**ip dhcp limit lease per interface**

RBE Client Side Encapsulation with QoS

The RBE Client Side Encapsulation with QoS feature integrates routed bridged encapsulation (RBE) with quality of service (QoS) features on the Cisco 800 and 1700 series routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RBE Client Side Encapsulation with QoS

To understand the RBE Client Side Encapsulation with QoS feature, you must be familiar with routed bridge encapsulation as described in the ATM Routed Bridge Encapsulation feature module introduced in Cisco IOS Release 12.1(2)T, and with QoS class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), and class-based marking and policing as described in the Cisco IOS Quality of Service Solutions Configuration Guide.

Information About RBE Client Side Encapsulation with QoS

RBE and QoS

The RBE Client Side Encapsulation with QoS feature provides secure connectivity to an ATM bridged network in which previously a broadband access server would not forward Address Resolution Protocol (ARP) requests or perform proxy ARP, and would respond to ARPs for its own IP address only. This feature combines RBE with QoS policy-based routing to provide security to the entire network. RBE was developed to address known issues with RFC1483 bridging such as broadcast storms and security.

From the network point of view, the ATM connection looks like a routed connection. Data traffic is received as RFC1483 packets, but are actually RFC1483 Ethernet or IEEE 802.3 frames. Instead of bridging the Ethernet or IEEE 802.3 frame, as in the case of regular RFC1483 bridging, the router routes on the Layer 3 header. With the exception of some cursory checks, the bridge header is ignored.

From an operational point of view, the router operates as if the routed-bridge interface were connected to an Ethernet LAN. RBE functions in the same way as half-bridging, except that it operates only over ATM. The operation is described in two ways: packets originating from the customer premises and packets destined for the customer premises.

For packets originating from the customer premises, the Ethernet header is skipped and the destination IP address is examined. If the destination IP address is in the route cache, the packet is fast switched to the outbound interface. If the destination IP address is not in the route cache, the packet is queued for process switching. In the process switch mode, the outbound interface through which the packet must be routed is found when software routines identifies it in the routing table. After the outbound interface is identified, the packet is routed on that interface. This routing occurs without the requirement for a bridge group or bridge group virtual interface (BVI).

For packets destined for the customer premises, the destination IP address of the packet is examined first. The destination interface is determined from the IP routing table. Next, the router checks the ARP table associated with that interface for a destination MAC address to place in the Ethernet header. If none is found, the router generates an ARP request for the destination IP address. The ARP request is forwarded to the destination interface only. This is in contrast to bridging, in which the ARP request is sent to all interfaces in the bridge group.

The RBE Client Side Encapsulation with QoS feature provides the ability, as an example, to pass packets to the network with a destination MAC address of 0.0.0.0 to populate the ARP on return traffic.

Low-Latency Queueing and Class-Based Weighted Fair Queueing

Low-latency queueing (LLQ) brings strict priority queueing to CBWFQ. Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued, thereby giving delay-sensitive data preferential treatment over other traffic.

Without LLQ, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic that is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The LLQ feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, LLQ enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue. To enqueue class traffic to the strict priority queue, you configure the **priority** command for the class after you specify the named class within a policy map. (Classes to which the **priority**command is applied are considered priority classes.) Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is enqueued to the same, single, strict priority queue.

One of the ways in which the strict priority queueing used within CBWFQ differs from its use outside CBWFQ is in the parameters it takes. Outside CBWFQ, by using the **ip rtp priority** command, you specify the range of User Datagram Protocol (UDP) ports whose voice traffic flows are to be given priority service. Using the **priority** command, because you can configure the priority status for a class within CBWFQ, you are no longer limited to a UDP port number to stipulate priority flows. Instead, all of the valid match criteria used to specify traffic for a class now apply to priority traffic. These methods of specifying traffic for a class include matching on access lists, protocols, and input interfaces. Moreover, within an access list you can specify that traffic matches are allowed based on the IP Differentiated Services Code Point (DSCP) value that is set using the first six bits of the Type of Service (ToS) byte in the IP header.

Class-Based Marking

In a traffic stream, a packet is classified based on the content of some portion of the packet header. The Behavior Aggregate (BA) classifier classifies packets based on the DSCP only. The Multi-field (MF) classifier selects packets based on the the value of the combination of one or more header fields, such as source address, destination address, Differentiated Services (DS) field (a replacement header field that supersedes the existing definitions of the IPv4 ToS octet and the IPv6 traffic class octet), protocol ID, source port and destination port numbers, and other information such as incoming interface and outgoing interface. The packet can be marked by a packet marker to set the DS field of a packet to a particular code point, adding the marked packet to a particular DS behavior aggregate.

Class-Based Policing

Class-based policing is applied when you attach a traffic policy containing a class-based policing configuration to an interface. A traffic policy is configured using the Modular Quality of Service Command-Line Interface (Modular QoS CLI).

Class-based policing allows you to control the maximum rate of traffic transmitted or received on an interface. Class-based policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most class-based policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). A packet is marked and these markings can be used to identify and classify traffic for downstream devices. In some cases, such as ATM Cell Loss Priority (CLP) marking or Frame Relay Discard Eligibility (DE) marking, the marking is used to classify traffic.

Use class-based policing to set the IP precedence or DSCP values for packets entering the network. Networking devices within your network can then use the adjusted IP precedence values to determine how the traffic should be treated. For example, the Weighted Random Early Detection (WRED) feature uses the IP precedence values to determine the probability that a packet will be dropped.

Use class-based policing to assign packets to a QoS group. The router uses the QoS group to determine how to prioritize packets within the router.

The Single Rate Three Color Marker (srTCM) meters an IP packet stream and marks its packets either conform, exceed, or violate. Marking is based on a Committed Information Rate (CIR) and two associated burst sizes, a Committed Burst Size (CBS) and an Excess Burst Size (EBS). A packet is marked "conform" if it does not exceed the CBS, marked "exceed" if it does exceed the CBS but not the EBS, and marked "violate" otherwise.

Additional References

The following sections provide references related to the RBE Client Side Encapsulation with QoS feature.

Related Documents

Related Topic	Document Title
Routed bridge encapsulation	• Configuring Broadband Access: PPP and Routed Bridge Encapsulation Configuring PPP over ATM " chapter in the Cisco IOS Wide-Area Networking Configuration Guide • ATM Routed Bridge Encapsulation feature module
Policy-based routing with QoS	• Class-Based Weighted Fair Queueing and Low Latency Queueing sections in the Cisco IOS Quality of Service Solutions Configuration Guide

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for RBE Client Side Encapsulation with QoS

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 RBE Client Side Encapsulation with QoS

Feature Name	Releases	Feature Information
RBE Client Side Encapsulation with QoS	12.4(2)T	The RBE Client Side Encapsulation with QoS feature integrates routed bridged encapsulation (RBE) with quality of service (QoS) features on the Cisco 800 and 1700 series routers. The following commands were introduced or modified: **atm route-bridged.**

Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

The Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature enables routed bridge encapsulation (RBE) over ATM permanent virtual circuit (PVC) bundles. This feature supports PVC bundle member selection based on the quality of service (QoS) group or on the type of service (ToS) or Multiprotocol Label Switching (MPLS) Experimental (EXP) bit in each packet over RBE interfaces. The PVC bundles carry RBE traffic configured on ATM point-to-point subinterfaces.

This feature also supports PVC bundle functionality for ATM adaptation layer 5 (AAL5) multiplexer (MUX) or Logical Link Control (LLC)/Subnetwork Access Protocol (SNAP) encapsulations and ATM PVC bundle scalability.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

The following restrictions apply to the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature:

- RBE over switched virtual circuit (SVC) bundles is not supported.
- SVC bundle member selection based on QoS groups is not supported.
- Fast switching is not supported (only Cisco Express Forwarding switching and process switching are supported).
- PVC bundle member selection based on QoS groups does not support distributed platforms.
- PVC bundle member selection based on QoS groups does not support bumping, protection, or PVC bundle incompleteness detection.

PVC bundles are supported under the following conditions (numbers are maximum per interface and per router):

- 1000 PVC bundles with AAL5 LLC/SNAP encapsulation, and each PVC bundle with four PVC bundle members
- 800 PVC bundles with two members each and with AAL5 LLC/SNAP encapsulation, and interfaces with 4000 PVCs overall (including PVC bundle members)

Information About Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

Benefits of Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

If the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature is not configured, you can make the PVC bundle member selection based on ToS bit settings (for IP packets) or EXP bit settings (for MPLS packets). With the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature configured, you can make the PVC bundle member selection based on the QoS group value associated with the packet on the ingress before route selection, or on the egress after selecting the adjacency. The packet's pak_type header is marked with the QoS group to use, based on the generic match criterion provided by the modular QoS (MQC) command-line interface (CLI).

The Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature gives you the flexibility to choose PVC bundle members based on various criteria. You can define any classification criterion for the traffic, mark the packets matching that criterion with the QoS group, and send them over a specific PVC bundle member to assign the appropriate quality of service to the corresponding class of traffic.

Memory Impact of Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

The additional memory required for configuring the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature does not exceed 50 bytes per PVC bundle.

Performance Impact of Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

The Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature impacts forwarding path performance when PVC bundles are configured with QoS groups. This impact results because, during forwarding, QoS groups must be mapped to the appropriate PVC bundle member index in the array of adjacencies associated with the PVC bundle adjacency.

This feature does not significantly increase CPU usage when traffic at line rates is sent over the PVC bundle (regardless of the selection criterion used for PVC bundle member selection).

How to Configure Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

Specifying the Method for Selecting PVC Bundle Members

Perform this task to specify the method of selection of PVC bundle members. You can specify one of two selection methods:

- QoS group--Use the QoS group value associated with each packet for selection of PVC bundle members.
- ToS or EXP--Use ToS bit settings of each packet (for IP packets) or EXP bit settings of each packet (for MPLS packets) for selection of PVC bundle members.

The selection methods are mutually exclusive. This means that when the selection method based on QoS groups is specified on any PVC bundle member, no other selection method is allowed on the same PVC bundle. Similarly, if the selection method based on ToS or EXP is specified on any PVC bundle member, no other selection method is allowed on the same PVC bundle.

Note

- You can change the selection method from QoS groups to ToS or EXP only if no PVC bundle member has QoS groups or Inverse Address Resolution Protocol (InverseARP) configured.
- You can change the selection method from ToS or EXP to QoS groups only if no PVC bundle member has precedence, protection, or bumping configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port*
4. **bundle** *bundle-name*
5. **selection-method** {**qos-group** | **tos-exp**}
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* / *port* **Example:** `Router(config)# interface atm 2/0`	Specifies the ATM interface type and enters interface configuration mode. To determine the correct form of the **interface atm** command, see your ATM network module, port adapter, or router documentation.
Step 4	**bundle** *bundle-name* **Example:** `Router(config-if)# bundle bundle-test`	Creates a PVC bundle or modifies an existing PVC bundle and enters ATM bundle configuration mode.
Step 5	**selection-method** {**qos-group** | **tos-exp**} **Example:** `Router(config-if-atm-bundle)# selection-method qos-group`	Specifies the method for selection of PVC bundle members.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if-atm-member)# end`	Ends the configuration session and returns to privileged EXEC mode.

Configuring the QoS Group-Based Method for Selection of PVC Bundle Members

Perform this task to configure the method for selection of PVC bundle members that is based on QoS groups.

You must associate a QoS group or groups with a PVC bundle member. You can specify a QoS group, a range of QoS groups, or any combination of QoS groups and ranges of QoS groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port*
4. **bundle** *bundle-name*
5. **selection-method qos-group**
6. **pvc** *vpi* / *vci*
7. **qos-group** *qos-groups*
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface atm** *slot* / *port* **Example:** `Router(config)# interface atm 2/0`	Specifies the ATM interface type and enters interface configuration mode. • To determine the correct form of the **interface atm** command, see your ATM network module, port adapter, or router documentation.
Step 4	**bundle** *bundle-name* **Example:** `Router(config-subif)# bundle bundle-test`	Creates a PVC bundle or modifies an existing PVC bundle and enters ATM bundle configuration mode.
Step 5	**selection-method qos-group** **Example:** `Router(config-if-atm-bundle)# selection-method qos-group`	Specifies the method for selection of PVC bundle members based on QoS group.
Step 6	**pvc** *vpi* / *vci* **Example:** `Router(config-if-atm-bundle)# pvc 1/32`	Creates an ATM PVC and enters ATM bundle-member configuration mode.
Step 7	**qos-group** *qos-groups* **Example:** `Router(config-if-atm-member)# qos-group 1`	Associates a QoS group or groups with the PVC bundle member.
Step 8	**end** **Example:** `Router(config-if-atm-member)# end`	Ends the configuration session and returns to privileged EXEC mode.

Configuring Explicit Inverse ARP PVC Selection for QoS Group-Based PVC Bundle Member Selection

Perform this task to configure explicit Inverse ARP for a PVC bundle member.

This procedure is optional and provides backward compatibility with existing PVC bundles, in which an Inverse ARP request is sent or expected to be received on the PVC bundle member with precedence 6. If a PVC bundle with selection based on QoS group is connected to an existing PVC bundle, you must follow this procedure to allow Inverse ARP to function. If you do not follow this procedure, Inverse ARP is sent over any of the available PVC bundle members.

Note You can enable Inverse ARP for a PVC bundle member only when using the QoS groups method for selecting PVC bundle members.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *slot* / *port*
4. **bundle** *bundle-name*
5. **selection-method qos-group**
6. **pvc** *vpi* / *vci*
7. **qos-group** *qos-groups*
8. **inarp-vc**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *slot* / *port* **Example:** `Router(config)# interface atm 2/0`	Specifies the ATM interface type and enters interface configuration mode. • To determine the correct form of the **interface atm** command, see your ATM network module, port adapter, or router documentation.
Step 4	**bundle** *bundle-name* **Example:** `Router(config-if)# bundle bundle-test`	Creates a bundle or modifies an existing bundle and enters ATM bundle configuration mode.

	Command or Action	Purpose
Step 5	**selection-method qos-group** **Example:** `Router(config-if-atm-bundle)# selection-method qos-group`	Specifies the method for selection of PVC bundle members based on QoS group.
Step 6	**pvc** *vpi* / *vci* **Example:** `Router(config-if-atm-bundle)# pvc 1/32`	Creates an ATM PVC and enters ATM bundle member configuration mode.
Step 7	**qos-group** *qos-groups* **Example:** `Router(config-if-atm-member)# qos-group 1`	Associates a QoS group or groups with the PVC bundle member.
Step 8	**inarp-vc** **Example:** `Router(config-if-atm-member)# inarp-vc`	Enables Inverse ARP for the PVC bundle member.
Step 9	**end** **Example:** `Router(config-if-atm-member)# end`	Ends the configuration session and returns to privileged EXEC mode.

Verifying Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

Perform this task to verify configuration of the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature:

SUMMARY STEPS

1. **enable**
2. **show atm vc**
3. **show interfaces**
4. **show interfaces virtual-access**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**show atm vc** **Example:** `Router# show atm vc`	Displays all ATM PVCs and SVCs and their traffic information.
Step 3	**show interfaces** **Example:** `Router# show interfaces`	Displays interleaving statistics. • Interleaving data is displayed only if interleaving occurs.
Step 4	**show interfaces virtual-access** **Example:** `Router# show interfaces virtual-access`	Displays multilink bundle information.

Configuration Examples for Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

- Specifying the Method for Selecting PVC Bundle Members Example, page 275
- Configuring the QoS Group-Based Method for Selection of PVC Bundle Members Example, page 276
- Configuring Explicit Inverse ARP PVC Selection for QoS Group-Based PVC Bundle Member Selection Example, page 276

Specifying the Method for Selecting PVC Bundle Members Example

The following example shows how to specify the method for selecting PVC bundle members:

```
interface atm 2/0
 bundle cisco
  selection-method qos-group
  end
```

Configuring the QoS Group-Based Method for Selection of PVC Bundle Members Example

The following example shows how to configure the QoS group-based method for selection of PVC bundle members:

```
interface atm 2/0
 bundle cisco
  selection-method qos-group
  pvc 35/56
  qos-group 1
  end
```

Configuring Explicit Inverse ARP PVC Selection for QoS Group-Based PVC Bundle Member Selection Example

The following example shows how to configure explicit Inverse ARP PVC selection for QoS group-based PVC bundle member selection:

```
interface atm 2/0
 bundle cisco
  selection-method qos-group
  pvc 1/32
  qos-group 1
  inarp-vc
  end
```

Additional References

The following sections provide references related to the Routed Bridge Encapsulation with ATM Virtual Circuit Bundles feature.

Related Documents

Related Topic	Document Title
Broadband access aggregation concepts	Understanding Broadband Access Aggregation
Preparing for broadband access aggregation tasks	Preparing for Broadband Access Aggregation
Broadband access aggregation and DSL commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
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 Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

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

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

Table 20 Feature Information for Routed Bridge Encapsulation with ATM Virtual Circuit Bundles

Feature Name	Releases	Feature Information
Routed Bridge Encapsulation with ATM Virtual Circuit Bundles	12.2(31)SB2 12.2(33)SRE 12.4(4)T	This feature enables RBE over ATM PVC bundles. This feature supports PVC bundle member selection based on the QoS group or on the ToS or MPLS EXP bit in each packet over RBE interfaces. The following command was introduced:**selection-method**.

Glossary

ARP --Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

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

bundle --A logical grouping of one or more physical interfaces using the formats and procedures of multilink Frame Relay. A bundle emulates a physical interface to the Frame Relay data link layer. The bundle is also referred to as the *MFR interface* .

Cisco Express Forwarding --Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

fast switching --Cisco feature in which a route cache expedites packet switching through a router.

Inverse ARP --Inverse Address Resolution Protocol (ARP). Method of building dynamic routes in a network. Allows an access server to discover the network address of a device associated with a virtual circuit.

MPLS --Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

MQC --modular QoS command-line interface (CLI). A CLI structure that lets you create traffic polices and attach them to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, and the QoS features in the traffic policy determine how to treat the classified traffic.

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

QoS --quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

RBE --routed bridge encapsulation. Process by which a stub-bridged segment is terminated on a point-to-point routed interface. Specifically, the router is routing on an IEEE 802.3 or Ethernet header carried over a point-to-point protocol, such as PPP, RFC 1483 ATM, or RFC 1490 Frame Relay.

SVC --switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. Called a switched virtual connection in ATM terminology.

ToS --type of service byte. Second byte in the IP header that indicates the desired quality of service for a specific datagram.

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

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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Configuring a Subscriber Service Switch Policy

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

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

Restrictions for Configuring a Subscriber Service Switch Policy

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

Information About the Subscriber Service Switch

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

Benefits of the Subscriber Service Switch

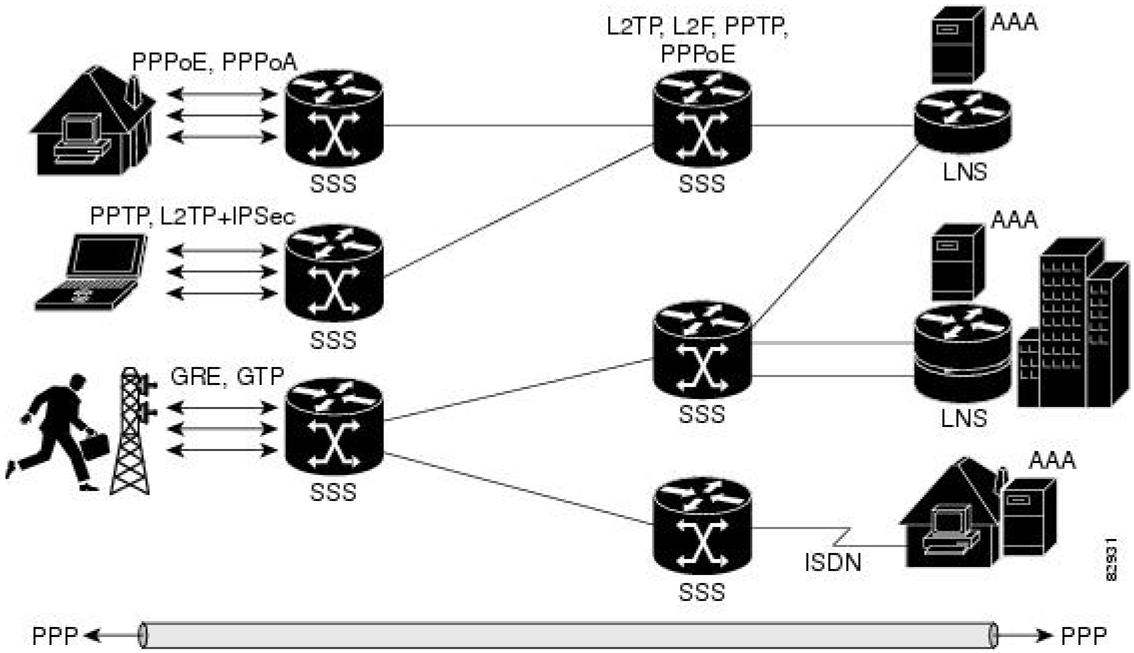
The Subscriber Service Switch provides the framework for the management and scalability of PPP sessions that are switched from one virtual PPP link to another. It gives Internet service providers (ISPs) the flexibility to determining which services to provide to subscribers, the number of subscribers,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

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

The figure below shows how the Subscriber Service Switch provides its own centralized switching path that bypasses the virtual-access-based switching available in previous releases. 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 17 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 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 **debug** commands that exist for troubleshooting PPP and other Layer 2 call operations. The table below lists some of these **debug** commands.

Table 21 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.
debug vpdn l2x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.

Command	Purpose
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 286
- Creating a RADIUS User Profile for Domain Preauthorization, page 287
- Enabling a Subscriber Service Switch Preauthorization, page 288
- Troubleshooting the Subscriber Service Switch, page 289

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 287

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 Security Configuration Guide for information about creating a RADIUS user profile.

Table 22 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 289

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 294. 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, page 292
- Domain Preauthorization RADIUS User Profile Example, page 292
- Subscriber Service Switch Preauthorization Example, page 292
- Verify Subscriber Service Switch Call Operation Example, page 292
- Troubleshooting the Subscriber Service Switch Examples, page 294
- Troubleshooting the Subscriber Service Switch Operation Example, page 294
- Troubleshooting the Subscriber Service Switch on the LAC--Normal Operation Example, page 295
- Troubleshooting the Subscriber Service Switch on the LAC--Authorization Failure Example, page 298

- Troubleshooting the Subscriber Service Switch on the LAC--Authentication Failure Example, page 299
- Troubleshooting the Subscriber Service Switch on the LNS--Normal Operation Example, page 302
- Troubleshooting the Subscriber Service Switch on the LNS--Tunnel Failure Example, page 304

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=net1.com,net2.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	"Wide-Area Networking Commands" chapter in the *Cisco IOS Wide-Area Networking 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 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 23 Feature Information for Configuring a Cisco Subscriber Service Switch Policy

Feature Name	Releases	Feature Configuration Information
Subscriber Service Switch	12.2(13)T 12.2(33)SRC	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. In Release 12.2(13)T, this feature was introduced. In Release 12.2(33)SRC, this feature was added to the SR release.

Subscriber Profile Support

The Subscriber Profile Support feature introduces new functionality for the Subscriber Service Switch architecture, a Cisco IOS subsystem that connects subscribers to network access services at Layer 2. This new functionality affects how the Subscriber Service Switch Manager determines a service for each subscriber with a combination of a policy and a service lookup model.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Configuring Subscriber Profile Support

Before configuring the Subscriber Profile Support feature, you need to be familiar with concepts introduced in the Cisco Release 12.2(13)T feature module *Subscriber Service Switch* , and with the authentication, authorization, and accounting (AAA) and PPP access processes.

Information About Subscriber Profile Support

New Call Management Support for Subscriber Service Switch Architecture

The Subscriber Service Switch architecture in Cisco IOS Release 12.3(4)T offers a significant improvement in scalability by providing the ability to bypass PPP when forwarding a call. Instead, call service selection is decided entirely by a Subscriber Service Switch Manager. Client call processes that terminate subscriber lines or receive subscriber calls send their requests for service direction to the Subscriber Service Switch Manager, which determines service based on service keys collected by the Subscriber Service Switch client and a preestablished call service policy. Examples of service keys are a NAS Port ID (network access server port identifier) and an unauthenticated PPP name. Refer to the *Subscriber Service Switch* feature module for more information about service keys.

The Subscriber Profile Support feature introduces the **subscriber profile** command and its **service** subcommands, which support the Subscriber Service Switch policy for searching a subscriber profile database for authorization data and determining the services that will be granted to the requesting customer.

How to Configure Subscriber Profile Support

The tasks described in this section assume that an operational network running the Subscriber Service Switch architecture has been configured.

Configuring VPDN Service for the Subscriber Service Switch Policy

In this task, you configure virtual private dial-up network (VPDN) service by directing the software to obtain the configuration from a predefined VPDN group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service 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.

	Command or Action	Purpose
Step 3	**subscriber profile** *profile-name* **Example:** `Router(config)#` **subscriber profile Domain1**	Names a Subscriber Service Switch policy for local searches of a subscriber profile database for authorization data when a AAA network authorization method list is configured, and enters subscriber profile configuration mode. **Note** Make sure that the **aaa authorization network default local** global configuration command is included in the configuration. (Do not use the **aaa authorization network default** command without the **local**keyword.)
Step 4	**service vpdn group** *vpdn-group-name* **Example:** `Router(config-sss-profile)# service vpdn group 1`	Provides VPDN service by obtaining the configuration from a VPDN group defined by the **vpdn-group** VPDN profile configuration command.
Step 5	**exit** **Example:** `Router(config-sss-profile)# exit`	Exits subscriber profile configuration mode.

• What to Do Next, page 311

What to Do Next

See the RADIUS Subscriber Service Switch Services Configuration, page 314 section for information about creating the script for the corresponding RADIUS AV pair Subscriber Service Switch attribute.

Configuring Local Termination Service for the Subscriber Service Switch Policy

In this task, you define local termination service for the Subscriber Service Switch policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service local**
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 Domain1`	Names a Subscriber Service Switch policy for local searches of a subscriber profile database for authorization data when a AAA network authorization method list is configured, and enters subscriber profile configuration mode. **Note** Make sure that the **aaa authorization network default local** global configuration command is included in the configuration. (Do not use the **aaa authorization network default** command without the **local**keyword.)
Step 4	**service local** **Example:** `Router(config-sss-profile)# service local`	Configures local termination, and is the default Subscriber Service Switch policy.
Step 5	**exit** **Example:** `Router(config-sss-profile)# exit`	Exits subscriber profile configuration mode.

• What to Do Next, page 312

What to Do Next

See the RADIUS Subscriber Service Switch Services Configuration, page 314 section for information about creating the script for the corresponding RADIUS AV pair Subscriber Service Switch attribute.

Configuring Denial of Service for the Subscriber Service Switch Policy

In this task, you configure a Subscriber Service Switch policy that denies service to a subscriber.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber profile** *profile-name*
4. **service deny**
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 Domain1`	Names a Subscriber Service Switch policy for local searches of a subscriber profile database for authorization data when a AAA network authorization method list is configured, and enters subscriber profile configuration mode. **Note** Make sure that the **aaa authorization network default local** global configuration command is included in the configuration. (Do not use the **aaa authorization network default** command without the **local**keyword.)
Step 4	**service deny** **Example:** `Router(config-sss-profile)# service deny`	Denies service to the subscriber.
Step 5	**exit** **Example:** `Router(config-sss-profile)# exit`	Exits subscriber profile configuration mode.

• What to Do Next, page 314

What to Do Next

See the RADIUS Subscriber Service Switch Services Configuration, page 314 section for information about creating the script for the corresponding RADIUS AV pair Subscriber Service Switch attribute.

RADIUS Subscriber Service Switch Services Configuration

The Cisco AV pairs have been extended to include Subscriber Service Switch service configuration. Subscriber Service Switch values are prefixed with "sss:", as follows:

cisco-avpair = "sss:sss-service=vpdn" cisco-avpair = "sss:sss-service=local" cisco-avpair = "sss:sss-service=deny"

Configuration Examples for Subscriber Profile Support

VPDN Service for the Subscriber Service Switch Policy Examples

The following example provides VPDN service to users in the domain cisco.com, and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to DNIS 1234567, and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node), and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile host:lac
 service vpdn group 1
```

Local Termination for the Subscriber Service Switch Policy Example

The following example provides local termination service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service local
```

Denial of Service for the Subscriber Service Switch Policy Example

The following example denies service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service deny
```

RADIUS Subscriber Service Support Profiles Examples

The following examples show typical RADIUS AV pair scripts to enable VPDN service and to define the service keys that are collected:

```
#
# Domain "cisco.com" users get VPDN service with the enclosed configuration.
#
cisco.com Password = "cisco"
User-Service-Type = Outbound-User,
cisco-avpair = "sss:sss-service=vpdn",
cisco-avpair = "vpdn:tunnel-id=nas-provider",
cisco-avpair = "vpdn:ip-addresses=10.0.3.96",
cisco-avpair = "vpdn:nas-password=secret1",
cisco-avpair = "vpdn:gw-password=secret2"
#
# Users with DNIS 1234567 get VPDN service with the enclosed configuration.
#
dnis:1234567 Password = "cisco"
User-Service-Type = Outbound-User,
cisco-avpair = "sss:sss-service=vpdn",
cisco-avpair = "vpdn:tunnel-id=nas-provider",
cisco-avpair = "vpdn:ip-addresses=10.0.3.96",
cisco-avpair = "vpdn:nas-password=secret1",
cisco-avpair = "vpdn:gw-password=secret2"
#
# Users on the remote tunnel (LAC) get VPDN service with the enclosed configuration.
#
host:lac Password = "cisco"
User-Service-Type = Outbound-User,
cisco-avpair = "sss:sss-service=vpdn",
cisco-avpair = "vpdn:tunnel-id=nas-provider",
cisco-avpair = "vpdn:ip-addresses=10.0.3.96",
cisco-avpair = "vpdn:nas-password=secret1",
cisco-avpair = "vpdn:gw-password=secret2"
```

Additional References

Related Documents

Related Topic	Document Title
AAA	*Cisco IOS Security Configuration Guide*; refer to " Part 1: Authentication, Authorization, and Accounting (AAA) "
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*

Related Topic	Document Title
Broadband access, PPPoE	*Cisco IOS Wide-Area Networking Configuration Guide*; refer to " Part 2: Broadband Access"
Broadband access, PPPoE, commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Wide-Area Networking Command Reference*
PPP	*Cisco IOS Dial Technologies Configuration Guide*; refer to "Part 9: PPP Configuration "
VPDN	*Cisco IOS Dial Technologies Configuration Guide*; refer to "Part 8: Virtual Templates, Profiles, and Networks "
PPP and VPDN commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Dial Technologies Command Reference*
Subscriber Service Switch	Subscriber Service Switch feature module

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for Subscriber Profile 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 24 Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Subscriber Profile Support	12.3(4)T	The Subscriber Profile Support feature introduces new functionality for the Subscriber Service Switch architecture, a Cisco IOS subsystem that connects subscribers to network access services at Layer 2. This new functionality affects how the Subscriber Service Switch Manager determines a service for each subscriber with a combination of a policy and a service lookup model. The following commands were introduced or modified: **service deny**, **service local**, **service vpdn group**, **subscriber profile**.

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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for Controlling Subscriber Bandwidth

The DBS feature does not support the following:

- Switched virtual circuits (SVC)
- PA-A1 or PA-A2 port adapters installed in a Cisco 7200 series router
- When changing QoS values dynamically on a VC, there will be some duration (typically milliseconds) during which traffic on the VC is dropped.

Information About Controlling Subscriber Bandwidth

- Benefits of Controlling Subscriber Bandwidth, page 320

Traffic-Shaping Parameters

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic-shaping parameters to be dynamically changed based on the RADIUS profile of a PPPoE or PPPoA user logging in on the PVC. If the user is the first user on a given PVC, the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all the sessions are selected as the PCR and SCR, respectively, of the VC.

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Traffic-shaping parameters can be locally configured by Cisco IOS command-line interface (CLI) in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic-shaping parameters that are CLI-configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overridden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a "QoS-management" string via vendor-specific attribute (VSA) 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for a particular user or domain. If the QoS specified for a domain or user cannot be applied on the PVC to which the session belongs, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** command to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you configure the **no dbs enable** command on a VC, additional sessions that are configured will display DBS-configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessions are already up on the VC, all sessions on that VC have DBS QoS parameters.

Benefits of Controlling Subscriber Bandwidth

DBS provides the following benefits:

- Wholesale service providers can provide different bandwidth options to their retail service provider customers, such as ISPs and enterprises.
- Subscribers can choose between enhanced and basic service, with a fixed billing plan for each service.

How to Control Subscriber Bandwidth

Configuring DBS Under a VC Class

Perform the following task to configure DBS under a VC class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **dbs enable**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**dbs enable** **Example:** `Router(config-vc-class)# dbs enable`	Applies DBS QoS parameters.

Configuring DBS on a PVC

Perform the following task to configure DBS for a PVC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *number* [**point-to-point** | **multipoint**]
4. **pvc** [*name*] *vpi* /*vci*
5. **dbs enable**
6. **protocol pppoe**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *number* [**point-to-point** | **multipoint**] **Example:** `Router(config)# interface atm 5/0.1 multipoint`	Specifies an ATM interface or subinterface and enters interface configuration mode.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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. Effective with Cisco IOS Release 12.2(28)SB, PPPOE termination is performed using the BBA 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    95   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 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 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 = "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"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco Subscriber Edge Services Manager	*Cisco Subscriber Edge Services Manager*
HTTP Redirect-Login on 6400 series routers	"Service Selection Gateway" chapter of the *Cisco 6400 Feature Guide* for Releases 12.1(5)DB and 12.1(5)DC
Cisco 6400	*Cisco 6400 Software Configuration Guide and Command Reference*
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*

Related Topic	Document Title
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 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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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 25 Feature Information for Controlling Subscriber Bandwidth

Feature Name	Releases	Feature Configuration Information
Dynamic Subscriber Bandwidth Selection (DBS)	12.2(4)B 12.2(13)T	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.

Configuring the Physical Subscriber Line for RADIUS Access and Accounting

Configuring a physical subscriber line for RADIUS Access and Accounting enables an L2TP access concentrator (LAC) and an L2TP network server (LNS) to forward RADIUS NAS-Port and NAS-Port-Type attribute values for PPP over ATM, PPPoE over ATM, and PPPoE over IEEE 802.1Q VLANs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Configuring the Physical Subscriber Line for RADIUS Access and Accounting

- RADIUS port identification for PPP requires the PPP extended NAS-Port format.
- You must perform the configuration procedures in the "Configuring RADIUS" chapter in the Cisco IOS Security Configuration Guide.
- You must perform the PPP over ATM configuration procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions" module.

- You must perform the PPPoE configuration procedures in the "Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module.

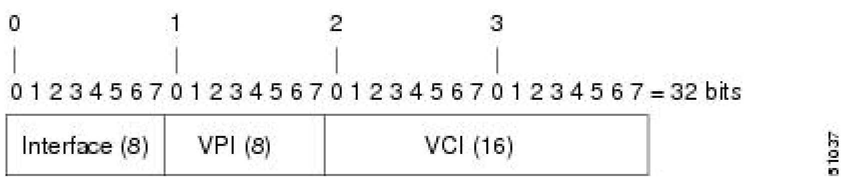
Note The PPP extended NAS-Port format increases the size of the NAS-Port attribute field to 32 bits and changes the NAS-Port attribute format to provide the RADIUS server with details about the ATM port, the virtual path identifier (VPI), the virtual channel identifier (VCI), and, for IEEE 802.1Q VLANs, the VLAN ID.

Information About Configuring the Physical Subscriber Line for RADIUS Access and Accounting

PPP over ATM and PPPoE over ATM NAS-Port Attribute Field Format

For PPP over ATM and PPP over ATM, the PPP extended format enables the NAS-Port attribute field to provide details about the ATM interface, VPI, and VCI. The figure below shows the format of the NAS-Port attribute field when the PPP extended NAS-Port format is configured and PPPoA over ATM or PPPoE over ATM is being used.

Figure 18 Format of the NAS-Port Attribute Field for PPP over ATM and PPPoE over ATM

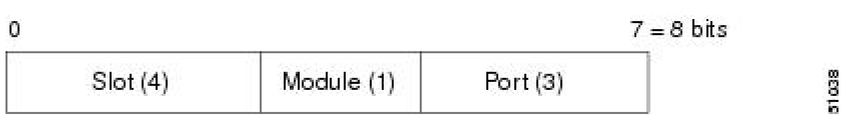


The interfaces, VPI, and VCI correspond to the interface and virtual circuit (VC) on which the ppp session entered the router.

Note For Cisco 6400 series routers, the interface, VPI, and VCI correspond to the interface and VC on which the session entered the Cisco 6400 node switch processor (NSP).

The figure below shows the format of the 8-bit interface field. For platforms that do not have slots or modules, the slot and module fields is 0.

Figure 19 Format of the Interface Field for PPP over ATM and PPPoE over ATM

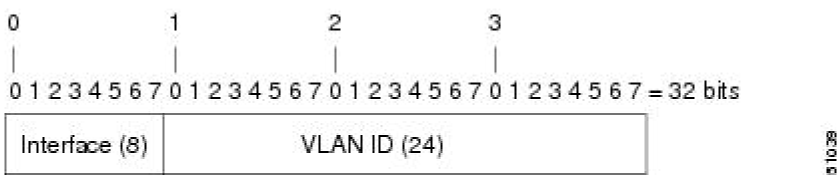


The NAS-Port-Type value for PPP over ATM and PPPoE over ATM is 5, which is the value for virtual port types.

PPPoE over IEEE 802.1Q VLANs Format

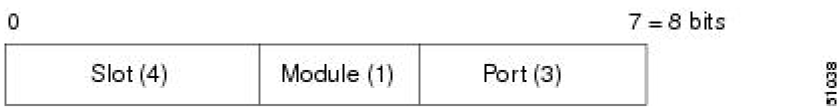
For PPPoE over 802.1Q VLANs, the PPP extended format provides details about the interface and the VLAN ID. The figure below shows the format of the NAS-Port attribute field when the PPP extended NAS-Port format is configured and PPPoE over an IEEE 802.1Q VLAN is being used.

Figure 20 Format of the NAS-Port Attribute Field for PPPoE over 802.1Q VLANs



The figure below shows the format of the 8-bit interface field. For platforms that do not have slots or modules, the slot and module fields will be 0.

Figure 21 Format of the Interface Field for PPPoE over 802.1Q VLANs



The NAS-Port-Type value for PPPoE over 802.1Q VLANs is 15.

How to Configure the Physical Subscriber Line for RADIUS Access and Accounting

- Configuring the LAC for RADIUS Port Identification for PPP, page 337
- Configuring the LNS for RADIUS Port Identification for PPP, page 338

Configuring the LAC for RADIUS Port Identification for PPP

Perform this task to configure the LAC for RADIUS port identification for PPP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
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	**radius-server attribute nas-port format d** **Example:** `Router(config)# radius-server attribute nas-port format d`	Specifies that PPP extended NAS-Port format that is used for RADIUS accounting.
Step 4	**end** **Example:** `Router(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

Configuring the LNS for RADIUS Port Identification for PPP

Perform this task to configure the LNS for RADIUS port identification for PPP.

Note In order for the LNS to forward PPP extended NAS-Port format values to the RADIUS server, both the LAC and the LNS must be Cisco routers running a Cisco IOS image that supports RADIUS port identification for PPP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute nas-port format d**
4. **vpdn aaa attribute nas-port vpdn-nas**
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	**radius-server attribute nas-port format d** **Example:** `Router(config)# radius-server attribute nas-port format d`	Specifies that PPP extended NAS-Port format that is used for RADIUS accounting.
Step 4	**vpdn aaa attribute nas-port vpdn-nas** **Example:** `Router(config)# vpdn aaa attribute nas-port vpdn-nas`	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.
Step 5	**end** **Example:** `Router(config-bba-group)# end`	Ends the configuration session and returns to privileged EXEC mode.

Configuration Examples for Identifying the Physical Subscriber Line

- RADIUS Port Identification for PPPoE over ATM Example, page 340
- RADIUS Port Identification for PPPoE over an 802.1Q VLAN Example, page 340
- LNS Configuration for RADIUS Port Identification for PPP Example, page 341

RADIUS Port Identification for PPPoE over ATM Example

The following example shows the configuration of the PPP extended NAS-Port format on an LAC using PPPoE over ATM:

```
vpdn enable
!
vpdn-group 1
 request-dialin
 protocol l2tp
```

domain vpn1

```
initiate-to ip 10.12.1.64  priority 1
 local name NAS1-1
!
virtual-template 1 pre-clone 20
virtual-template 2 pre-clone 20
!
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
```

!

```
interface ATM4/0.1 multipoint
 pvc 1/33
 encapsulation aal5snap
 protocol pppoe group vpn1
!
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
radius-server host 172.69.69.66 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key rad123
```

!

RADIUS Port Identification for PPPoE over an 802.1Q VLAN Example

The following example shows the configuration of the PPP extended NAS-Port format on an LAC running PPPoE over an 802.1Q VLAN:

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
```

sessions per-mac limit 2

```
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
```

```
 sessions per-mac limit 1 !
vc-class atm class-pppoe-global
 protocol pppoe
! !
interface FastEthernet2/0.2
 encapsulation dot1Q 2
 pppoe enable group vpn1
!
interface FastEthernet2/0.3
 encapsulation dot1Q 3
 pppoe enable group vpn2
!
```

aaa new-model

```
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
radius-server host 172.69.69.66 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
```

radius-server key rad123

LNS Configuration for RADIUS Port Identification for PPP Example

In the following example, the LNS is configured to recognize and forward PPP extended NAS-Port format values to the RADIUS server. The PPP extended NAS-Port format must also be configured on the LAC for this configuration to be effective.

```
vpdn enable
no vpdn logging
!
vpdn-group L2TP-tunnel
 accept-dialin
 protocol l2tp
 virtual-template 1
 terminate-from hostname lac1
 local name lns1
!
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
radius-server host 172.79.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key lns123
!
```

vpdn aaa attribute nas-port vpdn-nas

Additional References

The following sections provide references related to the Identifying the Physical Subscriber Line for RADIUS Access and Accounting feature.

Related Documents

Related Topic	Document Title
Configuring PPP over ATM sessions	"Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions" module
Configuring PPPoE sessions	"Providing Protocol Support for Broadband Access Aggregation of PPPoE Sessions" module
RADIUS configuration	"Configuring RADIUS" module of the*Cisco IOS Security Configuration Guide*
RADIUS attributes	"RADIUS Attributes" appendix to the *Cisco IOS Security Configuration Guide*
Tunneling configuration	*"Configuring Virtual Private Networks"* module of the *Cisco IOS Dial Technologies Configuration Guide*

Standards

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

MIBs

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

RFCs

RFC	Title
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 Identifying the Physical Subscriber Line for RADIUS Access and Accounting

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

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

Table 26 Feature Information for Identifying the Physical Subscriber Line for RADIUS Access and Accounting

Feature Name	Releases	Feature Information
RADIUS Port Identification	12.2(1) 12.2(33)SRC	Configuring RADIUS port identification for PPP enables an L2TP access concentrator (LAC) and an L2TP network server (LNS) to identify and forward RADIUS NAS-Port and NAS-Port-type attribute values for PPP over ATM, PPPoE over ATM, and PPPoE over IEEE 802.1Q VLANs. In 12.2(1), this feature was introduced. In 12.2(33)SRC, this feature was integrated into the SRC release.

1-Port ADSL WAN Interface Card

This feature module describes the 1-port Asymmetric Digital Subscriber Line (ADSL) Wide Area Network (WAN) Interface Card (WIC) feature. It describes the benefits of the feature, supported platforms, configuration, related documents, and provides command reference information.

The Cisco ADSL WAN interface cards are 1-port WAN interface cards (WIC) for Cisco modular access routers. These cards provide high-speed ADSL digital data transfer between a single customer premises equipment (CPE) subscriber and a central office.

Note ADSL is a last-mile access technology that uses an asymmetrical data rate over a single copper wire pair.

The ADSL WICs are available in two variations: ADSL over POTS (WIC-1ADSL), and ADSL over ISDN WAN with Dying Gasp support (WIC-1ADSL-I-DG). The following bullets summarize the features of each card:

- Cisco WIC-1ADSL--Provides ADSL services over ordinary telephone lines. It is compatible with the Alcatel Digital Subscriber Loop Access Multiplexer (DSLAM), the Cisco 6260 DSLAM with Flexi-line cards, and the Cisco 6130 DSLAM with Flexi-line cards.
- Cisco WIC-1ADSL-I-DG--Provides ADSL services in areas of the world that have extensive ISDN backbones already in place. It is compatible with ECI, Siemens, Alcatel, and Cisco DSLAMs that support ISDN.

All Cisco ADSL WICs support Asynchronous Transfer Mode (ATM) Adaptation Layer 2 (AAL2) for the Cisco 2600, Cisco 3600, and Cisco 3700 series only, and AAL5 for the those models as well as for the Cisco 1700. The cards support various classes of Quality of Service (QoS) for both voice and data.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for 1-Port ADSL WAN Interface Card

The Cisco ADSL WAN interface cards do not support dual latency, ADSL2, or ADSL2plus. When the ADSL link is intended to support both voice and data traffic simultaneously, the link should be configured for either all fast-path data or all interleave data, with an interleave depth of zero to ensure that latency is minimized. In addition, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.

Information About 1-Port ADSL WAN Interface Card

Benefits

Both Cisco ADSL WAN interface cards provide the following benefits:

- Enable business-class broadband service with voice integration, scalable performance, flexibility, and security
- Aggregate both ADSL and other transport options into a single box
- Provide ADSL high-speed digital data transmissions between CPE and the central office (CO)
- Support ATM AAL5 services and applications, ATM class of service (constant bit rate [CBR], variable bit rate-nonreal time [VBR-NRT], variable bit rate-real time [VBR-rt], and unspecified bit rate [UBR]), as well as up to 23 virtual circuits on a WIC in Cisco routers
- Provide ATM traffic management and QoS features to enable service providers to manage their core ATM network infrastructure.

The following benefits are specific to each card:

- Cisco WIC-1ADSL--Supports and complies with ANSI T1.413 Issue 2, and ITU G.992.1, Annex A (G.DMT for full-rate ADSL over POTS)
- Cisco WIC-1ADSL-I-DG--Allows the coexistence of ADSL and ISDN on the same local loop; supports and complies with ITU G.992.1, Annex B (G.DMT for full-rate ADSL over ISDN), ETSI 101-388, and the Deutsche Telekom U-R2 specification

How to Configure 1-Port ADSL WAN Interface Card

This section documents the new or changed Cisco IOS commands for configuring the Cisco ADSL WAN Interface Card feature. All other commands used to configure that feature are documented in the following publications:

- Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers
- The "Configuring ATM" section of the Cisco IOS Wide-Area Networking Configuration Guide
- The "ATM Commands" section of the Cisco IOS Wide-Area Networking Command Reference

See the following sections for configuration information:

Configuration Examples for 1-Port ADSL WAN Interface Card

Example Configuring Bridging on the ATM Interface with a Cisco ADSL WIC

The following sample shows a Cisco 1700 series router configured for bridging on the ATM interface with a Cisco ADSL WIC:

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname meltrack
!
no ip routing
!
interface ATM0
no ip address
atm vc-per-vp 256
    pvc 8/35
    encapsulation aal5snap
!
dsl operating-mode auto
bridge-group 1
!
interface FastEthernet0
no ip address
speed auto
bridge-group 1
!
ip classless
no ip http server
!
bridge 1 protocol ieee
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
```

end

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
ADSL WAN interface card on Cisco 1700 series routers	Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers
Release Notes	• *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.3(4)T* • *Caveats for Cisco IOS Release 12.3 T*
Interface card installation	*Cisco Interface Cards Hardware Installation Guide*
Configuring an ADSL WAN Interface Card	*Configuring an ADSL WAN Interface Card on Cisco 1700 Series Routers*
Enhanced Voice and QoS for ADSL and G.SHDSL	*Enhanced Voice and QoS for ADSL and G.SHDSL on Cisco 1700 Series, Cisco 2600 Series, and Cisco 3600 Series Routers*

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for 1-Port ADSL WAN Interface Card

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 1-Port ADSL WAN Interface Card

Feature Name	Releases	Feature Information
1-Port ADSL WAN Interface Card	12.1(3)XJ 12.2(2)T 12.2(13)ZH 12.2(15)ZJ 12.3(4)T	The Cisco ADSL WAN interface cards are 1-port WAN interface cards (WIC) for Cisco modular access routers. These cards provide high-speed ADSL digital data transfer between a single customer premises equipment (CPE) subscriber and a central office. Cisco WIC-1ADSL is supported on the following platforms: Cisco 1720, Cisco 1721, Cisco 1751, Cisco 1760, Cisco 2600, Cisco 2600XM, Cisco 2691, Cisco 3600, Cisco 3700 Cisco WIC-1ADSL-I-DG is supported on the following platforms: Cisco 1721, Cisco 1751, Cisco 1760, Cisco 2600XM, Cisco 2691, Cisco 3700 The following commands were introduced or modified: **dsl operating-mode .**

1-Port ADSL WAN Interface for the Cisco IAD2420 Series

This feature module describes the 1-port Asymmetric Digital Subscriber Line Wide Area Network (ADSL WAN) Interface for the Cisco IAD2420 Series. It describes the benefits of the new feature, supported platforms, configuration, related documents, and provides command reference information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for 1-Port ADSL WAN Interface

The ADSL WAN interface does not support dual latency. When the ADSL link is intended to support both voice and data traffic simultaneously, the link should be configured for either all fast-path data or all interleave data with an interleave depth of zero to insure that latency is minimized. In addition, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.

Information About 1-Port ADSL WAN Interface

ADSL WAN Interface

The ADSL 1-port WAN interface provides asymmetric digital subscriber line (ADSL) high-speed digital data transfer between a single customer premises equipment (CPE) subscriber and the central office.

The ADSL WAN interface is compatible with the Alcatel Digital Subscriber Line Access Multiplexer (DSLAM), the Cisco 6260 DSLAM with Flexi-line cards and the Cisco 6130 DSLAM with Flexi-line cards. It supports Asynchronous Transfer Mode (ATM) Adaptation Layer (AAL5 and AAL2) and various classes of Quality of Service (QoS) for both voice and data service.

Note ADSL is a last-mile access technology, which has an asymmetrical data rate running over a single copper wire pair.

The diagrams below show examples of typical deployment scenarios for the Cisco IAD2423.

Figure 22 ADSL WAN Interface with Analog FXS User Interface

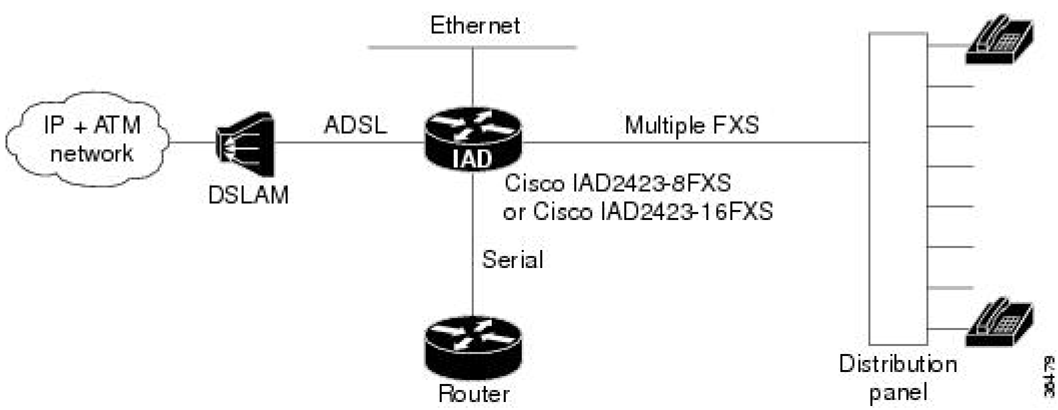


Figure 23 ADSL WAN Interface with T1 Interface to a PBX

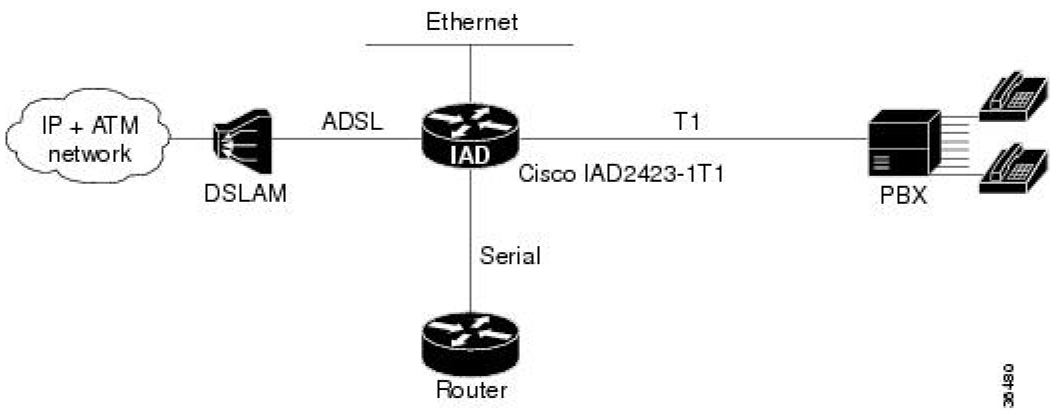
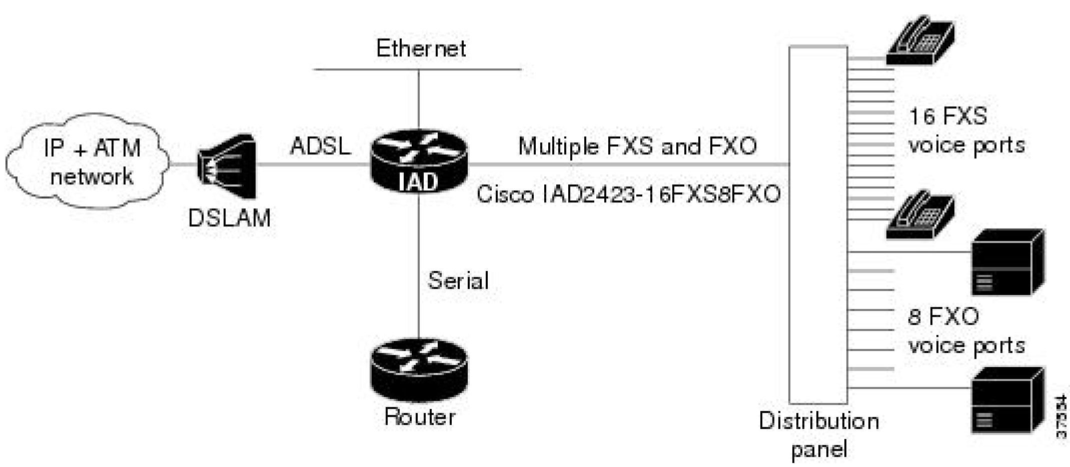


Figure 24 ADSL WAN INterface with FXS or FXO Interface



Benefits

- Enables business class broadband service with voice integration, scalable performance, flexibility, and security.
- Aggregates both ADSL and other transport options onto a single platform.
- Provides both POTS and ADSL high-speed digital data transmissions between the customer premise equipment (CPE) and the central office (CO).
- Supports ITU G.992.1 (or G.DMT, which specifies full-rate ADSL). Supports and complies with ANSI T1.413 issue 2, and ITU G.992.1 (G.DMT for full-rate ADSL).
- Supports ATM AAL5 and AAL2 services and applications, ATM class of service (constant bit rate [CBR], variable bit rate-nonreal time [VBR-NRT], variable bit rate-real time [VBR-rt], and unspecified bit rate [UBR]).
- Provides ATM traffic management and Quality of Service (QoS) features to enable service providers to manage their core ATM network infrastructures.

How to Configure the 1-Port ADSL WAN Interface

See the following sections for configuration tasks for the ADSL WAN interface feature. Each task in the list is identified as either required or optional.

Configuring the ADSL ATM Interface

If your Cisco IAD has an ADSL port, a default ATM configuration is automatically in effect when the Cisco IAD is first powered on. If your Cisco IAD has a T1-WAN port, a default ATM configuration takes effect when you enter the mode atm controller command. The default ATM configuration has the following operating parameters:

- ADSL port only.
    - Operating mode is auto--The ADSL interface operates in the mode specified by the remote DSL access multiplexer (DSLAM).
- T1-WAN port and ADSL port.
    - Maximum VPIs per VCI (atm vc-per-vc)--1024.
    - No IP address.
    - ATM UNI Version 4.0 is assigned.
    - ATM ILMI keepalive is disabled.
    - No ATM PVCs are configured

To configure the ADSL ATM interface, follow these steps:

SUMMARY STEPS

1. **enable**
2. **config terminal**
3. **controller t1 0**
4. **mode atm**
5. **exit**
6. **interface atm 0**
7. **ip address** *ip-address*
8. **atm uni-version** *version-number*
9. **atm ilmi-keepalive** *seconds*
10. **pvc** [*name*] *vpi/vci*
11. **protocol ip** *IP-address*
12. **vbr-rt** *peak-rate average-rate burst*
13. **encapsulation** {**aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5snap**}
14. **exit**
15. Repeat steps 9 through 13 for each ATM PVC to be configured.
16. **dsl operating-mode** {**ansi-dmt** | **auto** | **itu-dmt** | **splitterless**}
17. Router(config-if)# **no shutdown**
18. **exit**
19. **exit**
20. **show interface atm 0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**config terminal** **Example:** `Router# config terminal`	Enters global configuration mode.
Step 3	**controller t1 0**	Enter controller configuration mode and enter the controller number. The controller number for the T1-WAN port is 0. **Note** This step is only necessary if you have a T1 interface. `Router(config)# controller t1`

	Command or Action	Purpose
Step 4	**mode atm**	Enable ATM encapsulation and create logical ATM interface 0. Controller framing is automatically set to Extended SuperFrame (ESF). The linecode is automatically set to B8ZS. **Note** This step is only necessary if you have a T1 interface. `Router(config-ctrl)# mode atm`
Step 5	**exit** **Example:** `Router(config-ctrl)# exit`	Return to global configuration mode.
Step 6	**interface atm 0** **Example:** `Router(config)# interface atm 0`	Enters interface configuration mode for ATM 0.
Step 7	**ip address** *ip-address* **Example:** `Router(config-if)# ip address 10.2.0.1`	(Optional) Assigns an IP address to the ADSL ATM interface.
Step 8	**atm uni-version** *version-number* **Example:** `Router(config-if)# atm uni-version 2`	(Optional) Assign an ATM user network interface (UNI) version number.
Step 9	**atm ilmi-keepalive** *seconds* **Example:** `Router(config-if)# atm ilmi-keepalive`	(Optional) Enable Integrated Local Management Interface (ILMI) keepalives. **Note** The default value is 3 seconds.
Step 10	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)# pvc vc1 25/35`	Enters atm-virtual-circuit configuration mode, and configures a new permanent virtual circuit (PVC). Assigning a name is optional. **Note** The default traffic shaping is UBR and the default encapsulation is AAL5+LLC/SNAP.
Step 11	**protocol ip** *IP-address* **Example:** `Router(config-if-vc)# protocol ip 10.2.0.2`	(Optional) Enable IP and create a point-to-point IP address for the virtual circuit (VC).

	Command or Action	Purpose
Step 12	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-vc)# vbr-rt 672 672 512`	(Optional) Configure the PVC for real-time variable bit rate (VBR) traffic shaping. • Peak rate--peak information rate (PIR) • Average rate--average information rate (AIR) • Burst--burst size in cells
Step 13	**encapsulation** {**aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5snap**} **Example:** `Router(config-if-vc)# encapsulation aal5snap`	(Optional) Configure the ATM adaptation layer (AAL) and encapsulation type. • **aal1** for AAL1 • **aal2** for AAL2 • **aal5ciscoppp** for Cisco PPP over AAL5 • **aal5mux** for AAL5+MUX • **aal5nlpid** for AAL5+NLPID • **aal5snap** for AAL5+LLC/SNAP (default)
Step 14	**exit** **Example:** `Router(config-if-vc)# exit`	Exit for interface-ATM-VC configuration mode.
Step 15	Repeat steps 9 through 13 for each ATM PVC to be configured.	
Step 16	**dsl operating-mode** {**ansi-dmt** | **auto** | **itu-dmt** | **splitterless**} **Example:** `Router(config-if)# dsl operating-mode itu-dmt`	Configure the ADSL interface mode. • **ansi-dmt** --ANSI full rate mode per T1.413 (ITU G dmt Issue 1) • **auto** --Automatic detection mode (default) • **itu-dmt** --ITU full rate mode (ITU G dmt Issue 1) • **splitterless** --G.lite mode per ITU G.992.2
Step 17	Router(config-if)# **no shutdown** **Example:** `Router(config-if)# no shutdown`	Activate the ATM interface.
Step 18	**exit** **Example:** `Router(config-if)# exit`	Exit from the ATM interface configuration mode.

	Command or Action	Purpose
Step 19	**exit** **Example:** `Router(config)# exit`	Exit from the global configuration mode.
Step 20	**show interface atm 0** **Example:** `Router> show interface atm 0`	Verify the ATM interface configuration.

Configuring ATM for AAL2 Voice

This feature enables the Cisco IAD2423 to carry voice traffic (for example, telephone calls and faxes) over ATM networks using AAL2. AAL2 is the most bandwidth-efficient standards-based trunking method for transporting compressed voice, voice-band data, circuit-mode data, and frame-mode data over ATM infrastructures.

For configuration information, refer to the Cisco IOS Release 12.1(2)T feature module, Voice over ATM with AAL2 Trunking on Cisco MC3810 Series Concentrators, located on the World Wide Web at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_aal2v.htm

Configuring RSVP over an ATM Network

The RSVP-ATM Quality of Service (QoS) Interworking feature provides support for Controlled Load Service using RSVP over an ATM core network. This feature requires the ability to signal for establishment of switched virtual circuits (SVCs) across the ATM cloud in response to RSVP reservation messages. To meet this requirement, RSVP over ATM supports mapping of RSVP sessions to ATM SVCs.

RSVP-ATM QoS Interworking allows you to:

- Configure an interface or subinterface to dynamically create SVCs in response to RSVP reservation requests. To ensure defined QoS, these SVCs are established having QoS profiles consistent with the mapped RSVP flow specifications (flowspecs).
- Attach Distributed Weighted Random Early Detection (DWRED) group definitions to the PA-A3 ATM PA interface to support per-VC DWRED drop policy. Use of per-VC DWRED ensures that if packets must be dropped, then best-effort packets are dropped first and not those that conform to the appropriate QoS determined by the RSVP's token bucket.
- Configure the IP Precedence and type of service (ToS) values to be used for packets that conform to or exceed QoS profiles. As part of its input processing, RSVP uses the values that you specify to set the ToS and IP Precedence bits on incoming packets. If per-VC DWRED is configured, it then uses the ToS and IP Precedence bit settings on the output interface of the same router in determining which packets to drop. Also, interfaces on downstream routers use these settings in processing packets.

For configuration information, refer to, Configuring RSVP-ATM QoS Interworking, located on the World Wide Web at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt5/qcdrsatm.htm

Verifying the ATM Interface Configuration

To display ATM-specific information about an ATM interface, use the **show interface atm**privileged EXEC command.

```
Router# show interface atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC Atom1 (with Alcatel ADSL Module)
  Internet address is 15.15.15.3/24
  MTU 4470 bytes, sub MTU 4470, BW 832 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):, PVC mode
  512 maximum active VCs, 8 current VCCs
  VC idle disconnect time: 300 seconds
  Last input 3d23h, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Per VC Queueing
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     343791 packets input, 209797720 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5051487 packets output, 464110057 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

To display DSL information about an ADSL interface, use the show dsl interface atm privileged EXEC command.

```
Router# show dsl interface atm 0
Alcatel 20150 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.1 (G.DMT)
ITU STD NUM:     0x01                            0x1
Vendor ID:       'ALCB'                          'ALCB'
Vendor Specific: 0x0000                          0x0000
Vendor Country:  0x00                            0x0F
Capacity Used:   85%                             98%
Noise Margin:    13.5 dB                          7.0 dB
Output Power:     9.5 dBm                        12.0 dBm
Attenuation:      1.5 dB                          3.5 dB
Defect Status:   None                            None
Last Fail Code:  None
Selftest Result: 0x00
Subfunction:     0x15
Interrupts:      5940 (0 spurious)
PHY Access Err:  0
Activations:     1
SW Version:      3.670
FW Version:      0x1A04
                 Interleave             Fast    Interleave             Fast
Speed (kbps):             0             8128             0              864
Reed-Solomon EC:          0                0             0                0
CRC Errors:               0                0             0                7
Header Errors:            0                0             0                2
Bit Errors:               0                0
BER Valid sec:            0                0
BER Invalid sec:          0                0
DMT Bits Per Bin
00: 0 0 0 0 0 0 0 0 7 6 7 9 A B C C C
10: C C C C C C B B B B A 9 A 9 0 0
20: 0 0 0 0 0 0 2 2 3 4 4 5 6 6 7 7
30: 7 8 8 8 9 9 9 A A A A A A B B B
40: B B B B B B B B B B B A B B B B
50: B B B B B B B B B B B 2 B B B
```

```
60: B B B B B B B B B B B B B B B B
70: B B B B B B B B B B B B B B B B
80: B B B B B B B B B B B B B B B B
90: B B B B B B B B B B B B B B B B
A0: B B B B B B B B B B B B B B B B
B0: B B B B B B B B B B B B A B A A
C0: A A A A A A A A A A A A A A A A
D0: A A A A A A A A A A A 9 9 9 9 9
E0: 9 9 9 9 9 9 9 9 9 9 9 9 8 8 8 8
F0: 8 8 8 8 8 8 7 7 7 7 6 6 5 5 4 4
```

Troubleshooting Tips

To troubleshoot ADSL line problems, follow these steps:

SUMMARY STEPS

1. Check the carrier detect LED on the card. It will be off when the ADSL carrier is not detected. If it is off, it is a physical problem probably due to a bad cable or the problem with ADSL line or WAN service.
2. Make sure the ATM0 interface is not administratively shut down and the cable is good.
3. If the **show interface atm 0** command shows the interface as down, it means the Cisco IAD2423 sees the ADSL carrier but cannot train up with the Digital Subscriber Line Access Multiplexer (DSLAM) at the central office (CO).

DETAILED STEPS

Step 1 Check the carrier detect LED on the card. It will be off when the ADSL carrier is not detected. If it is off, it is a physical problem probably due to a bad cable or the problem with ADSL line or WAN service.

Step 2 Make sure the ATM0 interface is not administratively shut down and the cable is good.

Step 3 If the **show interface atm 0** command shows the interface as down, it means the Cisco IAD2423 sees the ADSL carrier but cannot train up with the Digital Subscriber Line Access Multiplexer (DSLAM) at the central office (CO). Turn on **debug atm events** (you need to turn on terminal monitor if you are in a telnet session to the router) and look at the output:

The ADSL activation stages are shown below:

STOP	in shutdown state
INIT	initialization
DLOAD_1	init and downloading first image
DLOAD_2	downloading second image
DO-OPEN	requesting activation with central office (CO)
SHOWTIME	activation succeeded

When in DO_OPEN state, look for the modem state for the progress information:

Modem state = 0x0	modem down
Modem state = 0x8	modem waiting to hear from CO

Modem state = 0x10	modem heard from CO, now training
Modem state = 0x20	modem activation completed, link is up

The following is a sample debug output:

Example:

```
*Mar  1 00:08:21.771: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_INIT]
*Mar  1 00:08:23.771: DSL: SM: [DMTDSL_INIT -> DMTDSL_DLOAD_1]
*Mar  1 00:08:23.771: DSL: Downloading asw_init_2_5_8.bin
*Mar  1 00:08:23.771: DSL: Downloaded 2 blocks... Finished!
*Mar  1 00:08:23.775: DSL: Sent command 0x14
*Mar  1 00:08:26.275: DSL: Received 1 timer events during wait
*Mar  1 00:08:27.711: DSL: Received response: 0x80
*Mar  1 00:08:27.715: DSL: SM: [DMTDSL_DLOAD_1 -> DMTDSL_DLOAD_2]
*Mar  1 00:08:27.715: DSL: Downloading asw_r2_5_8.bin
*Mar  1 00:08:27.791: DSL: Downloaded 100 blocks
*Mar  1 00:08:27.863: DSL: Downloaded 200 blocks
*Mar  1 00:08:27.935: DSL: Downloaded 300 blocks
*Mar  1 00:08:27.975: DSL: Downloaded 354 blocks... Finished!
*Mar  1 00:08:27.975: DSL: Sent command 0x14
*Mar  1 00:08:29.991: DSL: SM: [DMTDSL_DLOAD_2 -> DMTDSL_DO_OPEN]
*Mar  1 00:08:29.991: DSL: Send ADSL_OPEN command.
*Mar  1 00:08:29.991: DSL: Using subfunction 0x2
*Mar  1 00:08:29.991: DSL: Sent command 0x3
*Mar  1 00:08:32.491: DSL: 1: Modem state = 0x8
*Mar  1 00:08:34.991: DSL: 2: Modem state = 0x8
*Mar  1 00:08:37.491: DSL: 3: Modem state = 0x10
*Mar  1 00:08:39.991: DSL: 4: Modem state = 0x10
*Mar  1 00:08:42.491: DSL: 5: Modem state = 0x10
*Mar  1 00:08:44.991: DSL: 6: Modem state = 0x10
*Mar  1 00:08:46.003: DSL: Received response: 0x24
*Mar  1 00:08:46.003: DSL: Showtime!
*Mar  1 00:08:46.007: DSL: Sent command 0x11
*Mar  1 00:08:46.011: DSL: Received response: 0x61
*Mar  1 00:08:46.011: DSL: Read firmware revision 0x1A04
*Mar  1 00:08:46.011: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

Configuration Examples for 1-Port ADSL WAN Interface

- Example Cisco IAD2423 Configuration, page 361

Example Cisco IAD2423 Configuration

The following sample shows a Cisco IAD2423 configuration:

```
Building configuration...
Current configuration : 3187 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router
!
no logging buffered
logging rate-limit console 10 except errors
enable password mortify
!
network-clock base-rate 56k
network-clock-select 2 system(SCB)
ip subnet-zero
!
!
no ip finger
no ip domain-lookup
ip host newrouter 12.2.63.7
ip host motley 222.255.254.254
!
ip audit notify log
ip audit po max-events 100
frame-relay switching
!
voice-card 0
!
interface Ethernet0
 ip address 1.7.18.127 255.255.0.0
 ip helper-address 222.255.254.254
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no cdp enable
!
interface Serial0
 no ip address
 encapsulation frame-relay
 no ip route-cache
 no ip mroute-cache
 no keepalive
 shutdown
 no fair-queue
 no arp frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 200
  class fr801
 frame-relay ip rtp header-compression
!
interface ATM0
 ip address 15.15.15.3 255.255.255.0
 load-interval 30
 no atm ilmi-keepalive
 pvc 25/35
  encapsulation aal5snap
 !
 pvc 110/110
  encapsulation aal2
 !
 pvc 111/111
  protocol ip 15.15.15.2
  encapsulation aal5snap
 !
 pvc 120/120
  encapsulation aal2
 !
 dsl operating-mode itu-dmt
!
no ip classless
ip route 0.0.0.0 0.0.0.0 1.3.0.1
ip route 163.69.0.0 255.255.0.0 163.22.124.1
ip route 222.255.254.254 255.255.255.255 Ethernet0
no ip http server
!
!
map-class frame-relay fr801
 no frame-relay adaptive-shaping
```

```
 frame-relay cir 100000
 frame-relay bc 1000
 frame-relay mincir 100000
 frame-relay fair-queue
!
map-class frame-relay fr38
 frame-relay traffic-rate 1500000 1500000
 no frame-relay adaptive-shaping
 frame-relay cir 1500000
 frame-relay mincir 1500000
!
map-class frame-relay voice
!
map-class frame-relay 801
logging trap debugging
no cdp run
call rsvp-sync
!
voice-port 1/1
!
voice-port 1/2
!
voice-port 1/3
!
voice-port 1/4
!
voice-port 1/5
 connection plar 702
!
voice-port 1/6
 connection plar 702
!
mgcp modem passthrough voip mode ca
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1001 pots
 destination-pattern 1001
 port 1/1
!
dial-peer voice 2001 voatm
 destination-pattern 2001
 session protocol aal2-trunk
 session target ATM0 pvc 110/110 101
 signal-type trans
 codec aal2-profile custom 110 g711ulaw
 no vad
!
dial-peer voice 701 pots
 destination-pattern 701
 port 1/1
!
dial-peer voice 702 pots
 destination-pattern 702
 port 1/2
!
dial-peer voice 703 pots
 destination-pattern 703
 port 1/3
!
dial-peer voice 704 pots
 destination-pattern 704
 port 1/4
!
dial-peer voice 705 pots
 destination-pattern 705
 port 1/5
!
```

```
dial-peer voice 706 pots
 destination-pattern 706
 port 1/6
!
dial-peer voice 9999 voip
 destination-pattern 2222
 session target ipv4:12.12.12.2
 signal-type ext-signal
!
dial-peer voice 9998 voip
 destination-pattern 2223
 session target ipv4:123.123.123.123
 signal-type ext-signal
!
dial-peer voice 1000 voip
 signal-type ext-signal
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 transport input none
line aux 0
line 2 3
line vty 0 4
 privilege level 15
 no login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Release notes	• Release Notes for Cisco IAD2420 Series for Cisco IOS Release 12.1(5)XR • Cross-Platform Release Notes for Cisco IOS Release 12.2(4)T
IAD2420 configuration	• Cisco IAD2420 Series Software Configuration Guide • Cisco IAD2420 Series Hardware Installation Guide • Cisco IAD2420 Series Regulatory Compliance and Safety Information
Multiservice Applications configuration	• *Cisco IOS Multiservice Applications Configuration Guide* , Release 12.1 • *Cisco IOS Multiservice Applications Command Reference* , Release 12.1

Related Topic	Document Title
WAN configuration	*Cisco IOS Wide-Area Networking Configuration Guide* , Release 12.1

Standards

Standard	Title
ITU G.992.1	*G.DMT*
ITU G.992.2	*G.Lite*
T1.413 Issue 2	*ANSI*
AAL5	*ATM Adaptation Layer 5*
AAL2	*ATM Adaptation Layer 2*
UNI3.1 PVC	*ST2+ over ATM Protocol Specification - UNI 3.1 Version*

MIBs

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

RFCs

RFC	Title
RFC 1483	*Multiprotocol over ATM*
RFC 2364	*PPP over ATM*

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 1-Port ADSL WAN Interface

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

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

Table 28 Feature Information for 1-Port ADSL WAN Interface

Feature Name	Releases	Feature Information
1-Port ADSL WAN Interface	12.1(5)XR1 12.2(4)T	The ADSL 1-port WAN interface provides asymmetric digital subscriber line (ADSL) high-speed digital data transfer between a single customer premises equipment (CPE) subscriber and the central office. The ADSL WAN interface is compatible with the Alcatel Digital Subscriber Line Access Multiplexer (DSLAM), the Cisco 6260 DSLAM with Flexi-line cards and the Cisco 6130 DSLAM with Flexi-line cards. It supports Asynchronous Transfer Mode (ATM) Adaptation Layer (AAL5 and AAL2) and various classes of Quality of Service (QoS) for both voice and data service. The following platforms are supported: Cisco IAD2423-8FXS , Cisco IAD2423-16FXS, Cisco IAD2423-1T1, Cisco IAD2423-16FXS8FXO. The following commands were introduced or modified: **dsl operating-mode**, **show dsl interface atm .**

Glossary

AAL --ATM Adaptation Layer. ATM adaptation layer. Service-dependent sublayer of the data link layer. The AAL accepts data from different applications and presents it to the ATM layer in the form of 48-byte ATM payload segments.

AAL2 --ATM adaptation layer 2. ATM adaptation layer 2. One of four AALs recommended by the ITU-T. AAL2 is used for connection-oriented services that support a variable bit rate, such as some isochronous video and voice traffic.

AAL5 --ATM adaptation layer 5. ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented, VBR services, and is used predominantly for the transfer of classical IP over ATM and LANE traffic.

ADSL--Asymmetric Digital Subscriber Line.

ATM--Asynchronous Transfer Mode. Asynchronous Transfer Mode - International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. An internationally standardized implementation of cell relay technology, ATM represents the first worldwide standard to be embraced by the computer, communications, and entertainment industry. ATM is a high-bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique for data transmission that communicates all types of information (traditionally data, burst data, voice, video, image, and cell) over a common backbone using fixed cell lengths. ATM uses a 53-byte cell format that includes a 5-byte header and 48 bytes of payload. Because of the architecture, ATM has the capability to run from 45 Mbps using a DS3 to 2.5 Gbps using an OC-48.

broadband--Transmission system that multiplexes multiple independent signals onto one cable. In telecommunications terminology, any channel having a bandwidth greater than a voice-grade channel (4 kHz).

CBR--constant bit rate. QOS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.

CPE--customer premises equipment. Customer Premises Equipment. Devices that a subscriber is responsible for in order to make use of telecommunications. CPE includes PCs, telephones, TVs, scanners, and much more. These devices or terminating equipment---such as terminals, telephones, and modems---are generally supplied by the telephone company, installed at customer sites, and connected to the telephone company network.

CO--Central Office - Local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs. CO refers to the physical facility that contains the telephone switching system, transmission equipment, and other support systems that provide telephone and other telecommunications services to local telephone subscribers. There are numerous types of telephone switching systems, such as 1ESS, 4ESS, 5ESS, DMS 10/100/250/500, EAX2, or GTD5 that can be housed in a central office. The central office is not to be confused with the point of presence (POP) of the interexchange carrier, even though both perform many similar functions.

DSLAM--Digital Subscriber Line Access Multiplexer. A device that concentrates traffic in DSL implementations through a process of time-division multiplexing (TDM) at the CO or remote line shelf. This device is usually located in the CO for termination of multiple customer DSL devices.

DWRED--Distributed Weighted Random Early Detection. Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

ILMI--Interim Local Management Interface. Specification developed by the ATM Forum for incorporating network-management capabilities into the ATM UNI.

POTS--plain old telephone service. Basic analog telephone service, usually associated with residential or business subscribers.

PPP over ATM--Point-to-Point Protocol. A successor to SLIP, PPP provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.

PVC--permanent virtual circuit. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time.

QoS--quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

RSVP--Resource Reservation Protocol. The Resource Reservation Protocol is a network-control protocol that enables Internet applications to obtain special qualities of service (QoSs) for their data flows.

SVC--switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. Called a switched virtual connection in ATM terminology.

ToS--type of service. See COS.

UBR--unspecified bit rate. QOS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network, but there are no guarantees in terms of cell loss rate and delay.

UNI--User-Network Interface. ATM Forum specification that defines an interoperability standard for the interface between ATM-based products (a router or an ATM switch) located in a private network and the ATM switches located within the public carrier network.

VBR--variable bit rate. QOS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class.

VC--virtual circuit. Logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a virtual path identifier/virtual channel identifier (VPI/VCI) pair, and can be either a PVC or a SVC. Virtual circuits are used in Frame Relay and X.25. In ATM, a virtual circuit is called a virtual channel.

1-Port ADSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers

This document describes the 1-port Asymmetric Digital Subscriber Line (ADSL) WAN Interface Card (WIC) (WIC-1ADSL) feature for Cisco 2600 series and Cisco 3600 series routers in Cisco IOS Release xx.x(x)X. It describes the benefits of the new feature, supported platforms, configuration, related documents, and provides command reference information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for 1-Port ADSL WAN Interface Card

A 1-Port ADSL WIC must be installed in the router to match the DSL service to be configured.

Restrictions for 1-Port ADSL WAN Interface Card

- The ADSL WAN interface card does not support dual latency. When the ADSL link is intended to support both voice and data traffic simultaneously, the link should be configured for either all fast-path data or all interleave data with an interleave depth of zero to insure that latency is minimized. In addition, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.

- The ADSL WAN interface card does not support available bit rate (ABR) class of service (CoS).
- For the Cisco 2600 series routers, the ADSL WAN interface card should be inserted only into on-board WIC slots or 2W network modules. This card does not function properly in older network modules.
- For the Cisco 3600 series routers, the ADSL WAN interface card should be inserted only into on-board WIC slots or 2W, 1FE2W, 2FE2W, or 1FE1R2W network modules. This card does not function properly in older network modules.
- When using AAL2, analog voice is not supported. Voice calls should come through a digital voice card, such as the NM-HDV.
- VoATM is supported in both AAL2 and AAL5 modes on the Cisco 2600 series and Cisco 3600 series.
- VoATM AAL2 and AAL5 are supported only if voice and data use separate permanent virtual circuits (PVCs).
- VoATM AAL2 supports digital voice (T1/E1) only, while VoATM AAL5 supports both analog and digital voice.
- VoIP is not supported unless the ADSL WIC carries only voice traffic (with no data). The QoS features necessary for VoIP and data sharing the same PVC, or different PVCs on the same interface, are not supported yet. These features include LLQ, LFI, and tx-ring tuning.

Information About 1-Port ADSL WAN Interface Card

- ADSL WAN Interface Card, page 372

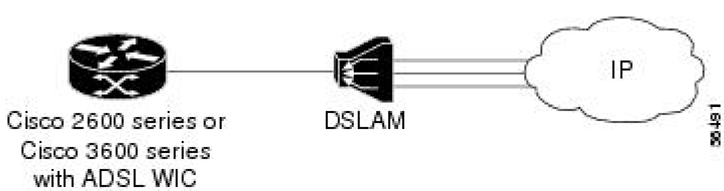
ADSL WAN Interface Card

The ADSL WAN interface card is a 1-port WAN interface card (WIC) for the Cisco 2600 series and Cisco 3600 series routers. The card provides asymmetric digital subscriber line (ADSL) high-speed digital data transfer between a single customer premises equipment (CPE) subscriber and the central office.

The ADSL WIC is compatible with the Alcatel Digital Subscriber Loop Access Multiplexer (DSLAM) and the Cisco 6130, Cisco 6160, and Cisco 6260 DSLAMs with Flexi-line cards. It supports Asynchronous Transfer Mode (ATM) Adaptation Layer 2 (AAL2) and AAL5 for the Cisco 2600 series and Cisco 3600 series platforms for both voice and data service.

The general topology is shown in the figure below.

Figure 25 General Topology for ADSL WIC



Note ADSL is a last-mile access technology, which has an asymmetrical data rate running over a single copper wire pair.

Benefits

- Enables business class broadband service with voice integration, scalable performance, flexibility, and security.
- Aggregates both ADSL and other transport options into a single box.
- Provides both POTS and ADSL high-speed digital data transmissions between the customer premises equipment (CPE) and the central office (CO).
- Supports ITU G.992.1 (or G.DMT, which specifies full-rate ADSL).
- Supports and complies with ANSI T1.413 issue 2, and ITU G.992.1 (G.DMT for full-rate ADSL).
- Supports ATM AAL2 and AAL5 services on the Cisco 2600 series and Cisco 3600 series platforms.
- Supports applications (including VoATM voice), ATM class of service (variable bit rate-nonreal time [VBR-NRT], variable bit rate-real time [VBR-rt], and unspecified bit rate [UBR]) and up to 23 virtual circuits on a WIC.
- Provides ATM traffic management to enable service providers to manage their core ATM network infrastructures.

How to Configure 1-Port ADSL WAN Interface Card

Features used on the ADSL WAN interface card must also be configured on the DSLAM. See the documentation for the specific DSLAM for information about configuring features.

Configuring the ADSL Port on the ADSL WAN Interface Card

To configure an ADSL port on the ADSL WAN interface card, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm slot/port**
4. **ip address***IP-address*
5. **pvc** [*name*] *vpi/vci*
6. **protocol ip***IP-address*
7. **vbr-rt***peak-rate average-rate burst*
8. **encapsulation aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap**
9. **exit**
10. **dsl operating-mode ansi-dmt** | **auto** | **itu-dmt** | **splitterless**
11. Router(config-if)# **no shutdown**
12. **exit**
13. **exit**
14. **show interface atm** *1/0*

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/port** **Example:** `Router(config)# interface atm0/1`	Enters ATM configuration mode for the ATM interface in the specified slot and port.
Step 4	**ip address***IP-address* **Example:** `Router(config-if)# ip address 10.1.1.1 255.0.0.0`	Assigns an IP address to the ADSL ATM interface.

	Command or Action	Purpose
Step 5	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)# pvc 10/100`	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM PVC by assigning a name (optional) and virtual path identifier (VPI)/virtual channel identifier (VCI) numbers. The default traffic shaping is UBR; the default encapsulation is AAL5+LLC/SNAP.
Step 6	**protocol ip***IP-address* **Example:** `Router(config-if-vc)# protocol ip 10.1.1.2 broadcast`	(Optional) Enables IP connectivity and create a point-to-point IP address for the virtual circuit (VC).
Step 7	**vbr-rt***peak-rate average-rate burst* **Example:** `Router(config-if-vc)# vbr-rt 672 672 512`	(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping. • *Peak rate* --Peak information rate (PIR) • *Average rate* --Average information rate (AIR) • *Burst* --Burst size in cells
Step 8	**encapsulation aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap** **Example:** `Router(config-if-vc)# encapsulation aal2`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • *aal2* --AAL2 • *aal5ciscoppp* --Cisco PPP over AAL5 • *aal5mux* --AAL5+MUX • *aal5nlpid* --AAL5+NLPID • *aal5snap* --AAL5+LLC/SNAP (the default)
Step 9	**exit** **Example:** `Router(config-if-vc)# exit`	Exits from interface-atm-vc configuration mode.
Step 10	**dsl operating-mode ansi-dmt** | **auto** | **itu-dmt** | **splitterless** **Example:** `Router(config-if)# dsl operating-mode ansi-dmt`	Configures the ADSL interface to operate in a specified mode: • *ansi-dmt* --ANSI full rate mode per T1.413 (ITU G.DMT Issue 1) • *auto* --Automatic detection mode • *itu-dmt* --ITU full rate mode (ITU G.DMT Issue 1) • *splitterless* --G.lite mode per ITU G.992.2 **Caution** This command is for testing or lab environments only. Using a configuration other than the default configuration for the DSL operating mode can lead to unpredictable behavior on the ADSL line.

	Command or Action	Purpose
Step 11	Router(config-if)# **no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the ATM interface.
Step 12	**exit** **Example:** `Router(config-if)# exit`	Exits from ATM interface configuration mode.
Step 13	**exit** **Example:** `Router(config)# exit`	Exits from global configuration mode.
Step 14	**show interface atm** *1/0* **Example:** `Router# show interface atm0/1`	Verifies the ATM interface configuration.

Verifying ATM Configuration

Use the following commands to verify configuration:

- To verify current configuration and to view the status for all controllers, use the show running-config command.
- To view ATM controller statistics, use the show controllers atm slot/port command.
- To verify the PVC status, use the show atm vc command. Make sure that active PVCs are up.
- To help identify ATM related events as they are generated, use the **debug atm events** command.
- To indicate what interfaces are having trouble, use the **debug atm errors** command.
- To identify an entry for the ATM interface you configured and to show an entry for the ATM slot/port you configured, use the **show ip route** command.
- To display the configured list of ATM static maps to remote hosts on an ATM network, use the show atm map command.
- To view the status of ATM interface, use the show interface atm slot/port command. Make sure that ATM slot/port and line protocol is up, as shown in the following example:

```
Router# show interface atm1/0
ATM1/0 is up, line protocol is up
  Hardware is DSLSAR (with Alcatel ADSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 800 Kbit, DLY 2560 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
```

```
  Encapsulation(s):AAL5 AAL2, PVC mode
  24 maximum active VCs, 256 VCs per VP, 2 current VCCs
  VC idle disconnect time:300 seconds
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters 03:16:00
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2527 packets input, 57116 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10798 packets output, 892801 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Router# show atm vc
            VCD /                                       Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC    Kbps   Kbps   Cells  Sts
1/0.3      2            9    36   PVC    MUX      UBR     800                 UP
1/0.2      1            9    37   PVC    SNAP     UBR     800                 UP
Router# show controllers atm 1/0
Interface ATM1/0 is up
  Hardware is DSLSAR (with Alcatel ADSL Module)
IDB:     62586758  Instance:6258E054  reg_dslsar:3C810000  wic_regs:3C810080
PHY Inst:62588490  Ser0Inst:62573074  Ser1Inst: 6257CBD8  us_bwidth:800
Slot:    1         Unit:     1         Subunit:  0         pkt Size:4496
VCperVP:256        max_vp:  256        max_vc:   65536     total vc:2
rct_size:65536      vpivcibit:16         connTblVCI:8         vpi_bits:8
vpvc_sel:3          enabled: 0          throttled:0
WIC    Register    Value      Notes
---------------    ---------- ----------
FPGA Dev ID (LB)   0x44       'D'
FPGA Dev ID (UB)   0x53       'S'
FPGA Revision      0x99
WIC Config Reg     0x45       WIC / VIC select = WIC;
                              CTRLE addr bit 8 = 1;
                              OK LED on;
                              LOOPBACK LED off;
                              CD LED on;
WIC Config Reg2    0x07       Gen bus error on bad ADSL access
Int 0 Enable Reg   0x03       ADSL normal interrupt enabled
                              ADSL error interrupt enabled
```

Configuration Examples for 1-Port ADSL WAN Interface Card

VoATM over AAL2 on the ATM Interface Example

The following example shows a Cisco 2600 series router configured for VoATM over AAL2 on the ATM interface with an ADSL card:

```
Router#
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
```

```
ip host host2 225.255.255.224
!
no mgcp timer receive-rtcp
call rsvp-sync
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1 type e&m-wink-start
 ds0-group 1 timeslots 2 type e&m-wink-start
.
.
.
ds0-group 23 timeslots 24 type e&m-wink-start
!
controller T1 1/1
 framing esf
 linecode b8zs
!
interface Ethernet0/0
 ip address 1.6.46.119 255.255.255.224
 half-duplex
 no cdp enable
!
interface Serial0/0
 no ip address
 shutdown
!
interface ATM0/1
 ip address 10.1.1.1 255.0.0.0
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 pvc 10/100
  vbr-rt 672 672 512
  encapsulation aal2
 !
 pvc 10/200
  protocol ip 10.1.1.2 broadcast
  encapsulation aal5snap
 !
 dsl operating-mode ansi-dmt
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 223.255.254.254 255.255.255.224 Ethernet0/0
no ip http server
!
!
snmp-server engineID local 000000090200003080477F20
snmp-server manager
!
voice-port 1/0:0
 local-alerting
 timeouts wait-release 3
 connection trunk 3001
!
voice-port 1/0:1
 local-alerting
 timeouts wait-release 3
 connection trunk 3002
.
.
.
voice-port 1/0:23
 local-alerting
 timeouts wait-release 3
 connection trunk 3024
```

```
 shutdown
!
dial-peer cor custom
!
dial-peer voice 3001 voatm
 destination-pattern 3001
 called-number 4001
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 31
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
dial-peer voice 3002 voatm
 destination-pattern 3002
 called-number 4002
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 32
 codec aal2-profile custom 100 g726r32
 no vad
!
dial-peer voice 3003 voatm
 destination-pattern 3003
 called-number 4003
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 33
 codec aal2-profile ITUT 7 g729abr8
 no vad
.
.
.
dial-peer voice 3024 voatm
 destination-pattern 3024
 called-number 3024
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 54
 codec aal2-profile ITUT 7 g729abr8
 no vad
!
dial-peer voice 1 pots
 destination-pattern 4001
 port 1/0:0
!
dial-peer voice 2 pots
 destination-pattern 4002
 port 1/0:1
.
.
.
dial-peer voice 24 pots
 destination-pattern 4024
 port 1/0:23
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
no scheduler allocate
end
```

VoATM over AAL5 on the ATM Interface Example

The following example shows a Cisco 2600 series router configured for VoATM over AAL5 on the ATM interface with an ADSL card.

```
Router#
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname u2621
!
no logging buffered
no logging buffered
logging rate-limit console 10 except errors
!
memory-size iomem 15
voice-card 1
!
ip subnet-zero
!
no ip finger
no ip domain-lookup
!
no mgcp timer receive-rtcp
call rsvp-sync
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
!
!
interface ATM0/0
 ip address 12.0.0.1 255.255.255.224
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 dsl operating-mode auto
 no fair-queue
!
!
interface FastEthernet0/0
 ip address 1.7.73.1 255.255.255.224
 duplex auto
 speed auto
!
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.224
 load-interval 30
 duplex auto
 speed auto
!
ip classless
ip route 223.255.254.0 255.255.255.224 FastEthernet0/0
no ip http server
!
!
snmp-server engineID local 0000000902000002163DB260
snmp-server packetsize 4096
snmp-server manager
!
voice-port 1/0:0
!
dial-peer cor custom
!
!
dial-peer voice 5 pots
 destination-pattern 777...
 port 1/0:0
 prefix 777
!
!
dial-peer voice 100 voatm
 destination-pattern 888....
 session target atm0/0 pvc 0/72
!
```

```
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Vice configuration	• *Cisco IOS Voice, Video, and Fax Configuration Guide* , Release 12.2 • *Cisco IOS Voice, Video, and Fax Command Reference* , Release 12.2
Configuring IP	*Cisco IOS IP Configuration Guide* , Release 12.2
Configuring ATM	"Configuring ATM" in the *Wide-Area Networking Configuration Guide, Release 12.2.*
Configuring a DSLAM	*Configuration Guide for Cisco DSLAMs with NI-2*
Installing Cisco 2600 series hardware	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm
Installing Cisco 3600 series hardware	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm

Standards

Standard	Title
ITU-T G.991.2	*Single-pair high-speed digital subscriber line (SHDSL) transceivers*
ANSI T1.413 issue 2	*ADSL features*
ITU 992.1	*G.DMT*

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for 1-Port ADSL WAN Interface Card

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

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

Table 29 Feature Information for 1-Port ADSL WAN Interface Card

Feature Name	Releases	Feature Information
1-Port ADSL WAN Interface Card	12.1(3)XJ 12.1(5)YB 12.2(2)T 12.2(4)T	This feature is supported on Cisco 2600 series and Cisco 3600 series routers. The following commands were introduced or modified: **show diag**, **show dsl interface atm**.

Glossary

ABR--available bit rate.

ADSL--asymmetric digital subscriber line (ADSL) available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

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

CLI--command line interface.

CO--central office, or local exchange (local switch), which terminates individual local telephone subscriber lines for switching, and connects to the public network. Known as a class 5 switch office. For example, 5ESS by Lucent and DMS 100 by Nortel.

CPE--customer premise equipment, including devices such as channel service units (CSUs)/data service units (DSUs), modems, and ISDN terminal adapters, required to provide an electromagnetic termination for wide-area network circuits before connecting to the router or access server. This equipment was historically provided by the telephone company, but is now typically provided by the customer in North American markets.

DSL--digital subscriber line available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

FXO--foreign exchange office. A FXO interface connects to a central office.

FXS--foreign exchange station: A FXS interface connects directly to a standard telephone, supplying ring voltage, dial tone, etc.

G.SHDSL--multirate symmetrical high-speed digital subscriber line.

PVC--permanent virtual circuit.

ADSL Support in IPv6

Asymmetric Digital Subscriber Line (ADSL) support in IPv6 provides the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on PPP links, per-user static routes, and ACLs.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for ADSL Support in IPv6

ADSL and dial deployment are available for interfaces with PPP encapsulation enabled, including PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), PPP over async, and PPP over ISDN.

ADSL Support in IPv6

Address Assignment for IPv6

A Cisco router configured with IPv6 will advertise its IPv6 prefixes on one or more interfaces, allowing IPv6 clients to automatically configure their addresses. In IPv6, address assignment is performed at the network layer, in contrast to IPv4 where a number of functions are handled in the PPP layer. The only function handled in IPv6 control protocol is the negotiation of a unique interface identifier. Everything else, including Domain Name Server (DNS) server discovery, is done within the IPv6 protocol itself.

Contrary to IPv4 address assignment, an IPv6 user will be assigned a prefix, not a single address. Typically, the ISP assigns a 64- or 48-bit prefix.

In IPv6, ISPs assign long-lived prefixes to users, which has some impact on the routing system. In typical IPv4 environments, each network access server (NAS) has a pool of 24-bit addresses and users get addresses from this pool when dialing in. If a user dials another point of presence (POP) or is connected to another NAS at the same POP, a different IPv4 address is assigned.

Addresses for IPv6 are assigned using two methods:

• Stateless Address Autoconfiguration, page 386

Stateless Address Autoconfiguration

Assigning addresses using the stateless address autoconfiguration method can be used only to assign 64-bit prefixes. Each user is assigned a 64-bit prefix, which is advertised to the user in a router advertisement (RA). All addresses are automatically configured based on the assigned prefix.

A typical scenario is to assign a separate 64-bit prefix per user; however, users can also be assigned a prefix from a shared pool of addresses. Using the shared pool limits addresses to only one address per user.

This method works best for the cases where the customer provider edge (CPE) router is a single PC or is limited to only one subnet. If the user has multiple subnets, Layer 2 (L2) bridging, multilink subnets or proxy RA can be used. The prefix advertised in the RA can come from an authorization, authentication, and accounting (AAA) server, which also provides the prefix attribute, can be manually configured, or can be allocated from a prefix pool.

The Framed-Interface-Id AAA attribute influences the choice of interface identifier for peers and, in combination with the prefix, the complete IPv6 address can be determined.

How to Configure ADSL Support in IPv6

• Configuring the NAS, page 386
• Configuring the Remote CE Router, page 390

Configuring the NAS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **aaa new-model**
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authorization configuration default** {**radius** | **tacacs+**
7. **show ipv6 route** [*ipv6-address* | *ipv6-prefix* / *prefix-length* | *protocol* | *interface-type interface-number*
8. **virtual-profile virtual-template** *number*
9. **interface serial** *controller-number* **:** *timeslot*
10. **encapsulation** *encapsulation-type*
11. **exit**
12. **dialer-group** *group-number*
13. **ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]
14. **interface virtual-template** *number*
15. **ipv6 enable**
16. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
17. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-53a`	Specifies the hostname for the network server.

	Command or Action	Purpose
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA server.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default if-needed group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 6	**aaa authorization configuration default** {**radius** | **tacacs+** **Example:** `Router(config)# aaa authorization configuration default radius`	Downloads configuration information from the AAA server.
Step 7	**show ipv6 route** [*ipv6-address* | *ipv6-prefix* / *prefix-length* | *protocol* | *interface-type interface-number* **Example:** `Router(config)# show ipv6 route`	Shows the routes installed by the previous commands.
Step 8	**virtual-profile virtual-template** *number* **Example:** `Router(config)# virtual-profile virtual-template 1`	Enables virtual profiles by virtual interface template.
Step 9	**interface serial** *controller-number* **:** *timeslot* **Example:** `Router(config)# interface serial 0:15`	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signaling, or robbed-bit signaling). This command also puts the router into interface configuration mode.
Step 10	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 12	**dialer-group** *group-number* **Example:** `Router(config)# dialer-group 1`	Controls access by configuring an interface to belong to a specific dialing group.
Step 13	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 14	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 15	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 16	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.

	Command or Action	Purpose
Step 17	**radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds* **Example:** `Router(config)# radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123`	Specifies a RADIUS server host.

Configuring the Remote CE Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **interface bri** *number* **.** *subinterface-number* [**multipoint** | **point-to-point**]
5. **encapsulation** *encapsulation-type*
6. **ipv6 address autoconfig** [**default**
7. **isdn switch-type** *switch-type*
8. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
9. **ppp multilink** [**bap** | **required**]
10. **exit**
11. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
12. **ipv6 route** *ipv6-prefix* / *prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-36a`	Specifies the hostname for the network server.
Step 4	**interface bri** *number* **.** *subinterface-number* [**multipoint** | **point-to-point**] **Example:** `Router(config)# interface bri 1.0`	Configures a BRI interface.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 6	**ipv6 address autoconfig** [**default** **Example:** `Router(config-if)# ipv6 address autoconfig`	Indicates that the IPv6 address will be generated automatically.
Step 7	**isdn switch-type** *switch-type* **Example:** `Router(config-if)# isdn switch-type basic-net3`	Specifies the central office switch type on the ISDN interface.
Step 8	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config-if)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

	Command or Action	Purpose
Step 9	**ppp multilink** [**bap** | **required**] **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 12	**ipv6 route** *ipv6-prefix* / *prefix-length* {*ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag* **Example:** `Router(config)# ipv6 route 2001:DB8::1/128 BRI1/0`	Establishes static IPv6 routes. • Use one command for each route.

Configuration Examples for ADSL Support in IPv6

Example: NAS Configuration

This configuration for the ISP NAS shows the configuration that supports access from the remote CE router.

```
hostname cust1-53a
  aaa new-model
  aaa authentication ppp default if-needed group radius
  aaa authorization network default group radius
  virtual-profile virtual-template 1
  interface Serial0:15
   encapsulation ppp
   dialer-group 1
   ppp authentication chap
  !
  interface Virtual-Template1
```

```
 ipv6 enable
!
dialer-list 1 protocol ipv6 permit
radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123
```

Example: Remote CE Router Configuration

This configuration for the remote customer edge router shows PPP encapsulation and IPv6 routes defined.

```
hostname cust-36a
  interface BRI1/0
   encapsulation ppp
   ipv6 enable
   isdn switch-type basic-net3
   ppp authentication chap optional
   ppp multilink
  !
  dialer-list 1 protocol ipv6 permit
  ipv6 route 2001:DB8::1/128 BRI1/0
  ipv6 route ::/0 2001:DB8::1
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco_IOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

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

Feature Information for ADSL Support in IPv6

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

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

Table 30 Feature Information for ADSL Support in IPv6

Feature Name	Releases	Feature Information
IPv6 ADSL and Dial Deployment Support	12.2(13)T	ADSL and dial deployment provide the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on PPP links, per-user static routes, and ACLs. The following commands were introduced or modified: **aaa authentication ppp**, **aaa authorization multicast default**, **aaa new-model**, **dialer-group**, **dialer-list**, **encapsulation**, **hostname**, **ipv6 address autoconfig**, **ipv6 route**, **isdn switch-type**, **ppp authentication**, **ppp multilink**, **radius-server host**, **show ipv6 route**, **virtual-profile virtual-template**.

Feature Name	Releases	Feature Information
IPv6 Access Services: PPPoA	12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoA.
IPv6 Access Services: PPPoE	12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoE.

ATM Mode for Two-Wire or Four-Wire SHDSL

This document describes the ATM Mode for Two-Wire or Four-Wire SHDSL feature on the Cisco 1700 series, Cisco 1800 series, Cisco 26xxXM, Cisco 2691, Cisco 2800, Cisco 3700 series, and Cisco 3800 series routers.

The ATM Mode for Two-Wire or Four-Wire SHDSL feature adds 4-wire support in fixed line-rate mode only on a WIC-1SHDSL-V2 or WIC-1SHDSL-V3 interface card. 2-wire mode supports 2-wire line-rate and auto line-rate. This feature builds on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card (WIC-1SHDSL). The 4-wire feature of G.991.2 doubles the bandwidth in ATM mode and increases usable distance over two pairs of wires.

The WIC-1SHDSL-V2 and WIC-1SHDSL-V3 support ATM on 2-wire and 4-wire line mode. Embedded Operation Channel (EOC) messages support for customer premises equipment (CPE) is provided for 2-wire and 4-wire modes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for ATM Mode for Two-Wire or Four-Wire SHDSL

- A G.SHDSL WIC must be installed in the router to match the DSL service to be configured.
- Minimum memory recommendations are shown in the table below.

Table 31 Minimum Memory Recommendations for ATM Mode for Two-Wire or Four-Wire SHDSL

Platform Name	Image Name	Flash Memory Recommended	DRAM Memory Recommended
Cisco 1700 Series	IOS IP BASE	16 MB	64 MB
Cisco 1800 Series	IOS IP BASE	16 MB	64 MB
Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM	IOS IP BASE	16 MB	64 MB
Cisco 2691	IOS IP BASE	32 MB	128 MB
Cisco 2800 Series	IOS IP BASE	32 MB	128 MB
Cisco 3725	IOS IP BASE	32 MB	128 MB
Cisco 3745	IOS IP BASE	32 MB	128 MB
Cisco 3800 Series	IOS IP BASE	32 MB	128 MB

Restrictions for ATM Mode for Two-Wire or Four-Wire SHDSL

- The *auto* parameter of the **line-mode** command on the WIC-1SHDSL-V2 is supported only in Cisco IOS Release 12.3(4)XG1 and later releases.
- The **standard** and **enhanced** keywords of the **line-mode 4-wire** command on the WIC-1SHDSL-V3 are supported only in Cisco IOS Release 12.4(2)XA and later releases.
- The WIC-1SHDSL-V2 and WIC-1SHDSL-V3 ATM mode for SHDSL does not support ATM adaptation layer 1 (AAL1) and/or circuit emulation service.
- ATM adaptation layer 2 (AAL2) is not supported on Cisco 1700 series, Cisco 1800 series, and Cisco 2801 routers.
- The ATM mode for SHDSL does not interface with AIM-ATM.
- The ATM mode for SHDSL does not support available bit rate (ABR) class of service (CoS).
- The ATM mode for SHDSL only supports 23 private virtual circuits (PVC) per WIC.
- The WIC-1SHDSL-V2 and WIC-1SHDSL-V3 should be inserted only into onboard WIC slots or NM-2W, NM-1FE2W, NM-1FE1R2W, NM-2FE2W, NM-1FE2W-V2, or NM-2FE2W-V2 network

modules. This WIC is not supported in NM-1E2W, NM-1E1R-2W, or NM-2E2W combination network modules.

- The WIC-1SHDSL and WIC-1SHDSL-V3 do not support T1/E1 mode.

Note The WIC-1SHDSL-V2 supports T1/E1 mode in 2-wire mode only, and only on certain routers with specific Cisco IOS images. For information about T1/E1 support on the WIC-1SHDSL-V2, see the T1/E1 Mode for SHDSL document.

Information About ATM Mode for Two-Wire or Four-Wire SHDSL

SHDSL Features

Supported SHDSL features are as follows:

- ITU G.991.2 support (full support for Annex A and B)
  - Dying gasp (ITU G.991.2) is supported.
  - Terminating wetting current is supported.
  - 2-wire mode supports speeds from 192 kbps to 2.304 Mbps in increments of 64 kbps in both fixed and auto line-rate.
  - 4-wire mode supports speeds from 384 kbps to 4.608 Mbps in increments of 128 kbps in fixed line-rate only and provides increased rate capability and greater reach.
- 4-wire mode supports both enhanced and standard mode.
- 2-wire and 4-wire auto-detection is supported.
- Diagnostic loopback mode is supported.
- Annex modes A-B, A-B-ANFP, and B-ANFP are supported

ATM Features

The supported ATM features in this release are:

- Provide ATM traffic management to enable service providers to manage their core ATM network infrastructures.
- Support ATM Class of Service features constant bit rate (CBR), variable bit rate-nonreal time (VBR-nrt), variable bit rate-real time (VBR-rt), unspecified bit rate (UBR), and unspecified bit rate plus (UBR+).
- Operate back-to-back or through a digital subscriber line access multiplexer (DSLAM).
- Provide toll-quality Voice over IP delivery over AAL5.
- Support VoATM over AAL2, but AAL2 is not supported on the Cisco 1700 series routers.

- Support VoATM over AAL5.
- Support FS OAM loopback and continuity check (oversubscription).

Interface and Controller Numbering on the Cisco 1721 Router

If a WIC-1SHDSL-V2 or WIC-1SHDSL-V3 is installed in a Cisco 1721 router, the interfaces and controllers are assigned numbers based on a numbering scheme that is different from the slot numbering scheme on other Cisco routers. This is because the Cisco 1721 router assigns only a slot number without also assigning a port number. Other Cisco routers typically use a slot and port number combination.

If a WIC-1SHDSL-V2 or WIC-1SHDSL-V3 (the DSL controller) is installed in slot 0, the ATM interfaces (ADSL/SHDSL) will be numbered relative to the DSL controller in slot 0. See the table below for examples of the slot numbering scheme on the Cisco 1721 router.

With an ATM card in slot 0, the WIC-1SHDSL-V2 or WIC-1SHDSL-V3 in slot 1 will be numbered relative to the number of ports in slot 0.

If both slots are occupied by DSL controllers, the logical interfaces configured on each controller will have the same number as the slot occupied by the DSL controller. All logical interfaces on the WIC-1SHDSL-V2 will have the same number as the DSL controller.

Table 32 Examples of Slot Numbering on the Cisco 1721 Router

Interface Cards and Controllers Installed	Slot Numbering Assignment

A WIC-1SHDSL-V2 or WIC-1SHDSL-V3 is in slot 0, and an ADSL/SHDSL WIC is in slot 1.	For WIC-1SHDSL-V2 or WIC-1SHDSL-V3:
	`controller dsl 0`
	`interface atm 0`
	For ADSL/SHDSL:
	`interface atm 1`

An ATM card is in slot 0, and a WIC-1SHDSL-V2 or WIC-1SHDSL-V3 is in slot 1. The WIC-1SHDSL-V2 or WIC-1SHDSL-V3 will be numbered relative to the ports in slot 0.	For ADSL/SHDSL:
	`interface atm 0`
	For WIC-1SHDSL-V2 or WIC-1SHDSL-V3:
	`controller dsl 1`
	`interface atm 1`

Interface Numbering on Cisco 2800 and Cisco 3800 Series Routers

This section describes the interface numbering scheme for Cisco 2800 and Cisco 3800 series routers. If an interface card is installed in a Cisco 2800 series or Cisco 3800 series router, the interfaces must use a triple-number scheme to identify them. This triple-number assignment is different from the standard interface numbering scheme on other Cisco routers.

The table below shows the interface numbering for the onboard Fast Ethernet ports and the interface slots on Cisco 2800 and Cisco 3800 series routers.

Table 33 Interface Numbering on Cisco 2800 Series and Cisco 3800 Series Router

Port/Slot	Interface Numbering	Example
Fast Ethernet ports (onboard)	0/0, 0/1	FE 0/0, 0/1
Slot 1	Slot 0/0/0	FE 0/0/0, 0/0/1, 0/0/2, 0/0/3
Slot 2	Slot 0/1/0	(Serial 2T) Serial 0/1/0, 0/1/1
Slot 3	Slot 0/2/0	FE 0/2/0
Slot 4	Slot 0/3/0	(G.SHDSL) ATM 0/3/0

How to Configure ATM Mode for Two-Wire or Four-Wire SHDSL

Configuring G.SHDSL Service

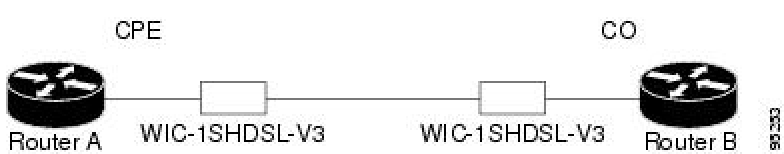
This section details how to configure the ATM Mode for Two-Wire or Four-Wire SHDSL feature for G.SHDSL service.

To configure G.SHDSL service in ATM mode on a Cisco router containing a G.SHDSL WIC, complete the steps in the Summary Steps or the Detailed Steps, beginning in global configuration mode.

The following list of prerequisites should be followed for this configuration:

- A G.SHDSL WIC must be installed in the router to match the DSL service to be configured.
- Routers may be set up for back-to-back operation as shown in the figure below, or they may be connected to a DSLAM.

Figure 26 Back-to-Back Setup



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller dsl** *slot* / *port*
4. **line-term** {**co** | **cpe**]
5. **dsl-mode shdsl symmetric annex** *mode*
6. **ignore-error-duration** *seconds*
7. **mode atm**
8. **For CPE:**
9. **line-rate** {*rate*| **auto**}
10. **exit**
11. **interface atm** *slot* /*port*
12. **ip address** *ip-address subnet-mask*
13. **atm ilmi-keepalive** [*seconds*]
14. **pvc** [*name*] *vpi/vci*
15. **protocol** *protocol* [*protocol-address*]
16. **vbr-rt** *peak-rate average-cell-rate burst*
17. **encapsulation aal2 | aal5ciscoppp | aal5mux | aal5nlpid | aal5snap| aal5autoppp**
18. **exit**
19. **exit**
20. **exit**
21. **show interface atm** *slot* / *port*
22. 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	**controller dsl** *slot* / *port* **Example:** `Router(config)# controller dsl 0/1`	Enters controller configuration mode. The keywords and arguments are as follows: • **dsl** --The type of controller. • *slot/port* --The backplane slot number and port number for the interface being configured.
Step 4	**line-term** {**co** | **cpe**] **Example:** `Router(config-controller)# line-term cpe`	Configures the DSL controller line termination as follows: • **co** --Central office. • **cpe** --Customer premises equipment.
Step 5	**dsl-mode shdsl symmetric annex** *mode* **Example:** `Router(config-controller)# dsl-mode shdsl symmetric annex A`	Sets the DSL operating mode parameters. The valid values are: • A: Supports Annex A of G.991.2 standard for North America. This is the default. • B: Supports Annex B of G.991.2 standard for Europe. • A-B: Supports Annex A or B. For CPE mode only. CO mode is not supported. Selected when the line trains. • A-B-ANFP: Supports Annex A or B-ANFP. For CPE mode only. CO mode is not supported. Selected when the line trains. • B-ANFP: Supports Annex B-ANFP.
Step 6	**ignore-error-duration** *seconds* **Example:** `Router(config-controller)# ignore-error-duration 15`	(Optional) Permits the router to ignore errors for a given amount of time while the line is being trained when connected to a controller with a different chipset type. • *seconds* --Number of seconds for which errors are ignored. The range is 15 to 30 seconds. If this value is omitted, an error message appears.
Step 7	**mode atm** **Example:** `Router(config-controller)# mode atm`	Enables ATM encapsulation and creates a logical ATM interface slot/port. **Note** If the **no mode atm** command is used to leave ATM mode, the router must be rebooted to clear the mode.

	Command or Action	Purpose

Step 8	**For CPE:**
	
	Example:
	
	line-mode [**4-wire** [**enhanced** | **standard**] | **2-wire** *line-number* | **auto**}
	
	Example:
	
	Example:
	
	For CO:
	
	Example:
	
	line-mode {**4-wire** [**enhanced** | **standard**] | **2-wire** *line-number*}
	
	Example:
	
	Example:
	
	`Router(config-controller)# line-mode 4-wire enhanced`
	
	Example:
		(Optional) Configures the controller to operate in 2-wire or 4-wire mode. The 2-wire mode is the default if this step is not configured or if the mode is not specified.
		
		• **2-wire** --Configures the controller to operate in 2-wire mode. This is the default if this step is omitted or if the mode is not specified.
		• **4-wire** --Configures the controller to operate in 4-wire mode.
		  ◦ **enhanced**--Configures 4-wire mode to exchange handshake status on both wire pairs. This is the default if the handshake mode is not specified.
		  ◦ **standard**--Configures 4-wire mode to exchange handshake status on the master wire pair only.
		• *line-number* --For 2-wire mode only, specifies the pair of wires used. Valid values are **line-zero** (default)or **line-one**. Line-zero choose RJ-11 pin 1 and pin 2; line-one chooses RJ-11 pin 3 and pin 4.
		• **auto** --Configures the line mode to be automatically detected for the CPE. This option is not available for configuring the CO.

	Command or Action	Purpose
Step 9	**line-rate** {*rate*| **auto**} **Example:** `Router(config-controller)# line-rate 1024`	**Note** Perform this step only if line-mode was not set to *auto* in Step 8. Specifies the DSL line rate for the SHDSL port. Auto mode is supported only in 2-wire mode. The argument is as follows: • auto--Allows the controller to select the rate. This option is available only in 2-wire mode. • *rate* --Sets the DSL line rate. The supported line rates are as follows: ◦ For 2-wire mode--192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, and 2304 ◦ For 4-wire mode--384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608. **Note** The configured line rate is the data rate available. Third-party equipment may use a line rate that includes an additional SHDSL overhead of 8 kbps for 2-wire mode or 16 kbps for 4-wire mode.
Step 10	**exit** **Example:** `Router(config-controller)# exit`	Exits controller configuration mode.
Step 11	**interface atm** *slot* /*port* **Example:** `Router(config)# interface atm 1/0`	Enters ATM configuration mode for interface ATM 0 in slot 1. The keywords and arguments are as follows: • *slot* --The backplane slot number for the interface being configured. • *port* --The backplane port number for the interface being configured. **Note** If a slot has two subslots for WIC modules and no ATM interface is present in subslot 0, the WIC will take ATM x/0 as its interface number even if placed in subslot 1 (ATMx/1). If a two-port WIC is present in subslot 0, the WIC will use ATM x/2 as its interface number. This subslot number is pertinent to all interface commands such as **show interface atm** and **show dsl interface atm**.
Step 12	**ip address** *ip-address subnet-mask* **Example:** `Router(config-if)# ip address 192.168.10.25 255.255.255.0`	Assigns an IP address to the DSL ATM interface.

	Command or Action	Purpose
Step 13	**atm ilmi-keepalive** [*seconds*] **Example:** `Router(config-if)# atm ilmi-keepalive 5`	(Optional) Enables Integrated Local Management Interface (ILMI) keepalives. • *seconds* --The number of seconds between keepalives. • If you enable ILMI keepalives without specifying the seconds, the default time interval is 3 seconds.
Step 14	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)# pvc [name] vpi/vci`	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM permanent virtual circuit (PVC) by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is an unspecified bit rate (UBR); the default encapsulation is AAL5+LLC/SNAP. • *name* --(Optional) Name of the PVC or map. The name can be up to 15 characters long. • *vpi/* -- ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a VPI value causes the VPI value to default to 0. Value ranges: • ◦ Cisco 2600 and Cisco 3600 series routers using Inverse Multiplexing for ATM (IMA): 0 to 15, 64 to 79, 128 to 143, and 192 to 207 The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. • *vci* --ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atm vc-per-vp** command. Typically, lower values from 0 to 31 are reserved for specific traffic (for example, F4 OAM, SVC signaling, ILMI, and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.
Step 15	**protocol** *protocol* [*protocol-address*] **Example:** `Router(config-if-vc)# protocol ip 192.168.0.4`	(Optional) Enables IP connectivity and creates a point-to-point IP address for the virtual circuit (VC). • *protocol* --Choose the **ip** protocol for this configuration. • *protocol-address* --Destination address that is being mapped to a permanent virtual circuit (PVC).

	Command or Action	Purpose
Step 16	**vbr-rt** *peak-rate average-cell-rate burst* **Example:** `Router(config-if-vc)# vbr-rt peak-rate average-cell-rate burst`	(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping. • *peak rate* --Peak cell rate (PCR). • *average-cell-rate* --Average cell rate (ACR). • *burst* --Burst size in cells.
Step 17	**encapsulation aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap**| **aal5autoppp** **Example:** `Router(config-if-vc)# encapsulation aal2`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • **aal2** --AAL2. • **aal5ciscoppp** --Cisco PPP over AAL5. • **aal5mux** --AAL5+MUX. • **aal5nlpid** --AAL5+NLPID. • **aal5snap** --AAL5+LLC/SNAP. • **aal5autoppp** --PPP autosense over AAL5. The default is **aal5snap**.
Step 18	**exit** **Example:** `Router(config-if-vc)# exit`	Exits interface-atm-vc configuration mode.
Step 19	**exit** **Example:** `Router(config-if)# exit`	Exits ATM interface configuration mode.
Step 20	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 21	**show interface atm** *slot* / *port* **Example:** `Router# show interface atm 1/0`	Displays the ATM interface configuration. The keywords and arguments are as follows: • *slot* --The backplane slot number for the interface being configured. • *port* --The backplane port number for the interface being configured.

	Command or Action	Purpose
Step 22	exit **Example:** `Router# exit`	Exits privileged EXEC mode.

• Examples, page 408
• What to Do Next, page 408

Examples

Example of the Configuration Before Configuring ATM Mode:

```
controller DSL 0/0
 line-term cpe
```

Example for 4-wire ATM, Annex B, and Line Rate 3200

```
controller DSL 0/1
 mode atm
 line-term cpe
 line-mode 4-wire enhanced
 dsl-mode shdsl symmetric annex B
 line-rate 3200
```

What to Do Next

The next task is to verify the ATM mode or DSL mode for the router.

Verifying the ATM Configuration

Perform the steps in this section to verify the ATM configuration.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. show controllers atm *slot*/*port*
4. show atm vc
5. debug atm events
6. debug atm errors
7. show interface atm *slot/port*
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	**show running-config** **Example:** `Router# show running-config`	Displays current running configuration and the status for all controllers.
Step 3	show controllers atm *slot*/*port* **Example:** `Router# show controllers atm 0/1`	Displays ATM controller statistics. The keywords and arguments are as follows: • *slot* --The backplane slot number for the interface being configured. • *port* --The backplane port number for the interface being configured.
Step 4	show atm vc **Example:** `Router# show atm vc`	Displays PVC status.
Step 5	debug atm events **Example:** `Router# debug atm events`	Identifies ATM-related events as they are generated.
Step 6	debug atm errors **Example:** `Router# debug atm errors`	Identifies interfaces with ATM errors.
Step 7	show interface atm *slot/port* **Example:** `Router# show interface atm 0/1`	Displays the status of the ATM interface. Ensure that the ATM slot/port and the line protocol are up. The keywords and arguments are as follows: • *slot* --The backplane slot number for the interface being configured. • *port* --The backplane port number for the interface being configured.

	Command or Action	Purpose
Step 8	exit **Example:** **Example:** `Router# exit`	Exits privileged EXEC mode.

- Examples, page 410
- What to Do Next, page 412

Examples

The following example shows how the **show interface atm**command is used and that the ATM slot/port and line protocol are up:

```
Router# show
 interfaces
 atm
 0/0
ATM0/0 is up, line protocol is up
  Hardware is DSLSAR
  MTU 4470 bytes, sub MTU 4470, BW 4608 Kbit, DLY 110 usec,
     reliability 0/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5 , PVC mode
  23 maximum active VCs, 256 VCs per VP, 1 current VCCs
  VC Auto Creation Disabled.
  VC idle disconnect time: 300 seconds
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Per VC Queueing
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
3725# show
 atm
 vc
           VCD /                                        Peak  Avg/Min
Burst
Interface  Name         VPI   VCI  Type   Encaps   SC   Kbps   Kbps
Cells  Sts
0/0.1      1              2   100  PVC    MUX      VBR    2000   2000 0   UP
0/1.1      1              2   100  PVC    SNAP     CBR    4608 UP
0/2.1      1              2   100  PVC    SNAP     VBR    4608   4200 0   UP
1/0.1      1              2   100  PVC    SNAP     VBR    4608   4608 0   UP
3725#
Router# show atm vc
            VCD /                                      Peak  Avg/Min Burst
Interface   Name        VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
1/0.3       2            9    36   PVC    MUX      UBR    800                UP
1/0.2       1            9    37   PVC    SNAP     UBR    800                UP
```

```
3725# show controllers atm
0
/
0
Interface: ATM0/0, Hardware: DSLSAR, State: up
IDB:     645F4B98  Instance: 645F646C  reg_dslsar:3C200000  wic_regs:
3C200080
PHY Inst:0         Ser0Inst: 645DFC8C  Ser1Inst:  645EA608  us_bwidth:4608
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 1
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enabled:  0         throttled: 0         cell drops: 0
Last Peridic Timer 00:44:26.872(2666872)
Parallel reads to TCQ:0  tx count reset = 0, periodic safe start = 0
Attempts to overwrite SCC txring: 0
Host Controller lockup recovery Info:
       recovery count1= 0, recovery count2= 0
Saved Host Controller Info to check any lockup:
      scc = 0, output_qcount = 0, head:0,
      buf addr = 0x00000000, serial outputs = 0
      scc = 1, output_qcount = 0, head:54,
      buf addr = 0x00000000, serial outputs = 212
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 0, current queue depth = 0, drops = 0, urun
cnt = 0, total cnt = 106
Serial idb tx count: AAL5: 0, RAW: 212, Drop count:AAL5: 0, RAW: 0
Host Controller Clock rate Info:
SCC Clockrates:
        SCC0 = 1000000 (ATM0/0)
        SCC1 = 8000000 (ATM0/0)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/2)
        SCC4 = 5300000 (ATM0/1)
        SCC5 = 8000000 (ATM0/2)
        SCC6 = 0
        SCC7 = 0
WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x53       'S'
FPGA Dev ID (UB)  0x4E       'N'
FPGA Revision     0xA7
WIC Config Reg    0x35       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 0;
                             NTR Enable = 0;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad G.SHDSL ATM/T1/E1 access
Int 0 Enable Reg  0x01       G.SHDSL ATM/T1/E1 normal interrupt enabled
                             G.SHDSL ATM/T1/E1 error interrupt disabled
DSLSAR Register   Value      Notes
---------------   ---------- ----------
sdram_refresh:    0x410FFFF  Expected value: 0x428xxxx
intr_event_reg:   0xC0       TMR.
intr_enable_reg:  0x13C      FIFOF.FBQE.RQAF.RPQAF.TSQAF.
config:           0x660D0A20 UTOPIA.RXEN.RegulateXmit.RMCell.TXEN.
                             Rx Buffer size: 8192.  RCT: Large, VPI Bits:
8.
status:           0x0
clkPerCell:       814121   (line rate: 4608 Kbps)
Pre-timer Count:  461
rcid_tableBase:   0x0
rct_base:         0x10000
tstBase1:         0x13C28    TST boot jump.
rawCellBase:      0x14300    (0/128) slots used.
rpq_base:         0x16000
tsqb(Tx Stat Q):  0x17000
fbq_base:         0x17880    (fbq_count: 128)
txChanQueue:      0x18000
rxBuffers:        0x30000
txBuffers:        0x130000
Lookup Error cnt: 0x0
```

```
Invalid Cell cnt: 0x0
SCCA Rx Errors:   0x0
SCCB Rx Errors:   0x0
Drop Pkt Count:   0x0
Total Tx Count:   0x0
Total Rx Count:   0x0
Timer:            0x73A141
DSLSAR Interrupts:0x0
       Last Addr:0x12E14
Router# show controllers
 atm

1
/
0
Interface ATM1/0 is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
IDB:    62586758  Instance:6258E054  reg_dslsar:3C810000  wic_regs:3C810080
PHY Inst:62588490  Ser0Inst:62573074  Ser1Inst: 6257CBD8  us_bwidth:800
Slot:   1         Unit:    1         Subunit:  0         pkt Size:4496
VCperVP:256       max_vp:  256       max_vc:   65536     total vc:2
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits:8
vpvc_sel:3         enabled: 0         throttled:0
WIC    Register   Value      Notes
---------------   ---------- ----------
WIC Config Reg    0x45       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 1;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad ADSL access
Int 0 Enable Reg  0x03       ADSL normal interrupt enabled
                             ADSL error interrupt enabled
```

What to Do Next

Verify the configuration using the detailed steps in the Verifying DSL Configuration, page 412.

Verifying DSL Configuration

Perform the steps in this section to verify the DSL configuration.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show controller dsl** *slot/port*
4. debug xdsl application
5. debug xdsl eoc
6. debug xdsl error
7. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the current running configuration and the status for all controllers.
Step 3	**show controller dsl** *slot/port* **Example:** `Router# show controller dsl 0/2`	Displays the DSL controller status. The keywords and arguments are as follows: • *slot* --The backplane slot number for the interface being configured. • *port* --The backplane port number for the interface being configured.
Step 4	debug xdsl application **Example:** `Router# debug dsl application`	Displays output of the DSL if the DSL does not come up.
Step 5	debug xdsl eoc **Example:** `Router# debug xdsl eoc`	Displays what is in the embedded operation channel (EOC) messages.
Step 6	debug xdsl error **Example:** `Router# debug xdsl error`	Displays error messages.

	Command or Action	Purpose
Step 7	exit **Example:** **Example:** `Router# exit`	Exits privileged EXEC mode.

• Examples, page 414

Examples

The following example shows how to verify 4-wire ATM mode in line zero (CPE):

```
Router# show controller dsl 0/0
DSL 0/0 controller UP
 Globespan xDSL controller chipset
 Line Mode: Four Wire
 DSL mode: Trained with SHDSL Annex B
 Frame mode: Utopia
 Configured Line rate: 4608Kbps
 Line Re-activated 9 times after system bootup
 LOSW Defect alarm: ACTIVE
 CRC per second alarm: ACTIVE
 Line termination: CPE
 FPGA Revision: 0xB3

Line 0 statistics

        Current 15 min counters
                CRC : 0 LOSW Defect : 0 ES : 0  SES : 0 UAS : 25

        Previous 15 min counters
                CRC : 0 LOSW Defect : 0 ES : 0  SES : 0 UAS : 0

        Current 24 hr counters
                CRC : 0 LOSW Defect : 4 ES : 0  SES : 0 UAS : 25

        Previous 24 hr counters
                CRC : 5 LOSW Defect : 4 ES : 1  SES : 0 UAS : 19

Line 1 statistics

        Current 15 min counters
                CRC : 0 LOSW Defect : 0 ES : 0  SES : 0 UAS : 25

        Previous 15 min counters
                CRC : 0 LOSW Defect : 0 ES : 0  SES : 0 UAS : 0

        Current 24 hr counters
                CRC : 0 LOSW Defect : 0 ES : 0  SES : 0 UAS : 25

        Previous 24 hr counters
                CRC : 6 LOSW Defect : 4 ES : 1  SES : 0 UAS : 19

 Line-0 status
 Chipset Version:  0
 Firmware Version:  R3.0.1
 Modem Status:  Data, Status 1
```

```
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.0 dB
 Transmit Power:  9.5 dB
 Receiver Gain:  19.5420 dB
 SNR Sampling:  37.6080 dB
 Line-1 status
 Chipset Version:  0
 Firmware Version:  R3.0.1
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.0 dB
 Transmit Power:  9.5 dB
 Receiver Gain:  19.5420 dB
 SNR Sampling:  37.6080 dB
 Dying Gasp: Present
```

Sample Output--Building Configuration

```
Router> show running-config
Current configuration : 3183 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3725
!
boot-start-marker
boot system flash c3725-is-mz.0424
boot system tftp shriv/c3725-is-mz.new 223.255.254.254
boot-end-marker
!
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
!
!
!
controller DSL 0/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 0/1
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
controller DSL 0/2
```

```
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 1/0
 mode atm
 line-term co
 line-mode 4-wire
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
!
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/0.1 point-to-point
 ip address 5.0.0.1 255.0.0.0
 pvc 2/100
  vbr-rt 2000 2000
  oam-pvc 0
  encapsulation aal5mux ip
 !
!
interface FastEthernet0/0
 ip address 1.3.208.25 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface ATM0/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM0/1.1 point-to-point
 ip address 6.0.0.1 255.0.0.0
 pvc 2/100
  cbr 4608
 !
!
interface FastEthernet0/1
 mac-address 0000.0000.0011
 ip address 70.0.0.2 255.0.0.0 secondary
 ip address 90.0.0.2 255.0.0.0 secondary
 ip address 50.0.0.2 255.0.0.0
 load-interval 30
 speed 100
 full-duplex
 no cdp enable
!
interface ATM0/2
 no ip address
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/2.1 point-to-point
 ip address 7.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4200
 !
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
```

```
!
interface ATM1/0.1 point-to-point
 ip address 8.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4608
 !
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 172.19.163.44
ip classless
ip route 60.0.0.0 255.0.0.0 ATM1/0.1
ip route 80.0.0.0 255.0.0.0 ATM0/1.1
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0
ip route 223.255.254.254 255.255.255.255 1.3.0.1
ip http server
!
!
access-list 101 permit ip host 20.0.0.2 host 20.0.0.1
snmp-server community public RO
snmp-server enable traps tty
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
end
```

Troubleshooting Tasks

The following commands verify hardware on the router:

- **show version** --Lists the modules installed in the router. If DSL controllers are installed, the output displays the following line:
    - 1 DSL controller --Indicates one DSL controller is installed in the router

and one of the following lines:

- ◦ 1 ATM network interface(s) --If the DSL controller is configured for mode ATM

    ◦ 1 Channelized T1/PRI port(s) --If the DSL controller is configured for mode T1
- **show controllers atm** --Displays the ATM controller status and statistics. The sample below shows the output in ATM mode. Actual output may vary depending on the router and the configuration.

```
Router# show controllers atm

0
/
0
Interface: ATM0/0, Hardware: DSLSAR, State: up
IDB:     645F4B98  Instance: 645F646C  reg_dslsar:3C200000  wic_regs: 3C200080
PHY Inst:0         Ser0Inst: 645DFC8C  Ser1Inst:  645EA608  us_bwidth:4608
Slot:    0         Unit:     0         Subunit:   0         pkt Size: 4528
VCperVP: 256       max_vp:   256       max_vc:    65536     total vc: 1
rct_size:65536     vpivcibit:16        connTblVCI:8         vpi_bits: 8
vpvc_sel:3         enabled:  0         throttled: 0         cell drops: 0
Last Peridic Timer 00:44:26.872(2666872)
Parallel reads to TCQ:0  tx count reset = 0, periodic safe start = 0
Attempts to overwrite SCC txring: 0
Host Controller lockup recovery Info:
       recovery count1= 0, recovery count2= 0
Saved Host Controller Info to check any lockup:
      scc = 0, output_qcount = 0, head:0,
      buf addr = 0x00000000, serial outputs = 0
      scc = 1, output_qcount = 0, head:54,
      buf addr = 0x00000000, serial outputs = 212
Serial idb(AAL5) output_qcount:0 max:40
Serial idb(RAW) output_qcount:0, max:40
Sar ctrl queue: max depth = 0, current queue depth = 0, drops = 0, urun
cnt = 0, total cnt = 106
Serial idb tx count: AAL5: 0, RAW: 212, Drop count:AAL5: 0, RAW: 0
Host Controller Clock rate Info:
SCC Clockrates:
        SCC0 = 1000000 (ATM0/0)
        SCC1 = 8000000 (ATM0/0)
        SCC2 = 1000000 (ATM0/1)
        SCC3 = 1000000 (ATM0/2)
        SCC4 = 5300000 (ATM0/1)
        SCC5 = 8000000 (ATM0/2)
        SCC6 = 0
        SCC7 = 0
WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x53       'S'
FPGA Dev ID (UB)  0x4E       'N'
FPGA Revision     0xA7
WIC Config Reg    0x35       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 0;
                             NTR Enable = 0;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad G.SHDSL ATM/T1/E1 access
Int 0 Enable Reg  0x01       G.SHDSL ATM/T1/E1 normal interrupt enabled
                             G.SHDSL ATM/T1/E1 error interrupt disabled
DSLSAR Register   Value      Notes
---------------   ---------- ----------
sdram_refresh:    0x410FFFF  Expected value: 0x428xxxx
intr_event_reg:   0xC0       TMR.
intr_enable_reg:  0x13C      FIFOF.FBQE.RQAF.RPQAF.TSQAF.
config:           0x660D0A20 UTOPIA.RXEN.RegulateXmit.RMCell.TXEN.
                             Rx Buffer size: 8192.  RCT: Large, VPI Bits: 8.
status:           0x0
clkPerCell:       814121   (line rate: 4608 Kbps)
Pre-timer Count:  461
rcid_tableBase:   0x0
rct_base:         0x10000
tstBase1:         0x13C28    TST boot jump.
rawCellBase:      0x14300    (0/128) slots used.
rpq_base:         0x16000
tsqb(Tx Stat Q):  0x17000
fbq_base:         0x17880    (fbq_count: 128)
```

```
txChanQueue:      0x18000
rxBuffers:        0x30000
txBuffers:        0x130000
Lookup Error cnt: 0x0
Invalid Cell cnt: 0x0
SCCA Rx Errors:   0x0
SCCB Rx Errors:   0x0
Drop Pkt Count:   0x0
Total Tx Count:   0x0
Total Rx Count:   0x0
Timer:            0x73A141
DSLSAR Interrupts:0x0
       Last Addr:0x12E14
```

- **show controllers dsl--** Displays the DSL controller status and statistics. The sample below shows the output in T1 mode. Actual output may vary depending on the router and the configuration.

```
Router# show controllers dsl

0
/
0
 DSL 0/0 controller UP
 Globespan xDSL controller chipset
 DSL mode: SHDSL Annex B
 Frame mode: Utopia
 Configured Line rate: 4608Kbps
 Line Re-activated 5 times after system bootup
 LOSW Defect alarm: ACTIVE
 CRC per second alarm: ACTIVE
 Line termination: CO
 FPGA Revision: 0xA7
Line 0 statistics
        Current 15 min CRC: 679
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 5
        Current 15 min SES: 5
        Current 15 min UAS: 441
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0
Line 1 statistics
        Current 15 min CRC: 577
        Current 15 min LOSW Defect: 8
        Current 15 min ES: 7
        Current 15 min SES: 4
        Current 15 min UAS: 455
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0
 Line-0 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.600 dB
 Transmit Power:  8.5 dB
 Receiver Gain:  21.420 dB
 SNR Sampling:  39.3690 dB
 Line-1 status
 Chipset Version:  1
 Firmware Version:  A29733
 Modem Status:  Data, Status 1
 Last Fail Mode:  No Failure status:0x0
 Line rate:  2312 Kbps
```

```
Framer Sync Status: In Sync
Rcv Clock Status: In the Range
Loop Attenuation:  0.4294966256 dB
Transmit Power:  8.5 dB
Receiver Gain:  21.420 dB
SNR Sampling:  39.1570 dB
Dying Gasp: Present
```

- **debug xdsl application** --Displays output from the xDSL to see what is happening if the DSL does not come up. When the debug xdsl application command is used, resources and the buffer are used and will impact operation.

```
Router# debug xdsl application

xDSL application debugging is on
Router#
Apr 23 06:01:26.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.720: DSL 0/0 process_get_wakeup
Apr 23 06:01:27.720: DSL 0/0 xdsl_process_boolean_events
XDSL_LINE_UP_EVENT:
Apr 23 06:01:28.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:29.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:30.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:31.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:32.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:33.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:34.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:34.476: DSL 0/0   SNR Sampling: 42.8370 dB
Apr 23 06:01:35.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:35.476: DSL 0/0   SNR Sampling: 41.9650 dB
Apr 23 06:01:36.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:36.476: DSL 0/0   SNR Sampling: 41.2400 dB
Apr 23 06:01:37.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:37.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:01:37.476: DSL 0/0 xdsl_background_process: one_second_timer triggers download
Apr 23 06:01:37.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:37.476: DSL 0/0 xdsl_background_process:Download boolean event received
Apr 23 06:01:37.476: DSL 0/0 xdsl_controller_reset: cdb-state=down
Apr 23 06:01:37.476: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to down
Apr 23 06:01:38.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:39.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:40.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:41.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:42.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:43.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:44.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:45.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:46.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:47.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:48.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:49.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:50.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:51.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:52.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:53.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:54.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:55.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:56.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.796: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.796: DSL 0/0 xdsl_process_boolean_events
XDSL_LINE_UP_EVENT:
Apr 23 06:01:57.812: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.812: DSL 0/0 xdsl_background_process: XDSL link up boolean event received
Apr 23 06:01:57.812:  DSL 0/0 controller Link up! line rate: 4608 Kbps
Apr 23 06:01:57.812: DSL 0/0 xdsl_controller_reset: cdb-state=up
Apr 23 06:01:57.812: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
Apr 23 06:01:57.812: DSL 0/0
Apr 23 06:01:57.812:  Dslsar data rate 4608
Apr 23 06:01:57.816: DSL 0/0 TipRing 1, Xmit_Power Val 85, xmit_power 8.5
Apr 23 06:01:57.816: DSL 0/0 Mode 2, BW 4608, power_base_value 145, power_backoff 6
```

```
Apr 23 06:01:57.912: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.916: DSL 0/0 process_get_wakeup
Apr 23 06:01:57.916: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.008: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.008: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.012: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.012: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.104: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.104: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.108: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.108: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.200: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.204: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:01:58.208: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.296: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.392: DSL 0/0 process_get_wakeup
Apr 23 06:01:58.476: DSL 0/0 process_get_wakeup
Apr 23 06:01:59.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:00.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:01.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.476: DSL 0/0 process_get_wakeup
Router#
Router#
Apr 23 06:02:02.920: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.920: DSL 0/0 process_get_wakeup
Apr 23 06:02:02.920: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.016: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:03.020: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.112: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.208: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.304: DSL 0/0 process_get_wakeup
Apr 23 06:02:03.476: DSL 0/0 process_get_wakeup
Router#
Router#
Apr 23 06:02:04.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:04.476: DSL 0/0   SNR Sampling: 42.3790 dB
Apr 23 06:02:04.476: DSL 0/0   SNR Sampling: 42.8370 dB
Router#
Apr 23 06:02:04.476: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
Apr 23 06:02:05.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:05.476: DSL 0/0   SNR Sampling: 41.5880 dB
Apr 23 06:02:05.476: DSL 0/0   SNR Sampling: 42.3790 dB
Apr 23 06:02:05.476: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed
state to up
Router#
Router#
Apr 23 06:02:06.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:06.476: DSL 0/0   SNR Sampling: 40.9180 dB
Apr 23 06:02:06.476: DSL 0/0   SNR Sampling: 41.5880 dB
Apr 23 06:02:07.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:02:07.476: DSL 0/0   SNR Sampling: 41.2400 dBu all
Apr 23 06:02:07.912: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.912: DSL 0/0 process_get_wakeup
Apr 23 06:02:07.912: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.008: DSL 0/0 xdsl_background_process: EOC boolean event received
Apr 23 06:02:08.016: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.104: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.200: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.296: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:08.476: DSL 0/0
All possible debugging has been turned off
Router#
Router#
```

```
Router#
Router#  SNR Sampling: 40.750 dB
Apr 23 06:02:08.476: DSL 0/0   SNR Sampling: 40.6180 dB
Apr 23 06:02:09.476: DSL 0/0 process_get_wakeup
Apr 23 06:02:09.476: DSL 0/0   SNR Sampling: 39.5920 dB
Apr 23 06:02:09.476: DSL 0/0   SNR Sampling: 40.3380 dB
```

- **debug xdsl driver** --Displays what is happening when the drivers are being downloaded and installed. The following example displays a sample output from the **debug xdsl driver**command:
  - 4-wire mode:

```
Router# debug xdsl driver
xDSL driver debugging is on
Router#
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1 framer intr_status 0xC1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 2/0 framer intr_status 0xC4
01:04:18: DSL 2/0 framer intr_status 0xC1
01:04:18: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1 framer intr_status 0xC4
01:04:18: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2
01:04:18: DSL 0/2 framer intr_status 0xC1  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:18: DSL 0/2 framer intr_status 0xC4
01:04:18: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:18: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/1 framer intr_status 0xC1
01:04:19: DSL 0/1  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/1  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 2/0 framer intr_status 0xC1
01:04:19: DSL 2/0  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 2/0  xdsl_gsi_int_disable(false):: 0x1
01:04:19: DSL 0/2 framer intr_status 0xC1
```

```
01:04:19: DSL 0/2  xdsl_gsi_int_disable(true):: 0x0
01:04:19: DSL 0/2  xdsl_gsi_int_disable(false):: 0x1
01:04:22: DSL 0/0  dsp interrupt-download next block for line-0
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-1
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-0
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:22: DSL 0/0  dsp interrupt-download next block for line-1
01:04:22: DSL 0/0 framer intr_status 0xC0
01:04:23: DSL 0/0  dsp interrupt-download next block for line-0
01:04:23: DSL 0/0 DSP interrupt disabled
01:04:23: DSL 0/0  Download completed for line-0
01:04:23: DSL 0/0 framer intr_status 0xC0
01:04:23: DSL 0/0  dsp interrupt-download next block for line-1
01:04:23: DSL 0/0 DSP interrupt disabled
01:04:23: DSL 0/0  Download completed for line-1
01:04:23: DSL 0/0 Framer interrupt enabled
01:04:23: DSL 0/0 framer intr_status 0xC0
01:04:23:  DSL 0/0 controller Link up! line rate: 4608 Kbps
01:04:23: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
01:04:23: DSL 0/0 framer intr_status 0xC4
01:04:23: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
01:04:23: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
01:04:23: DSL 0/0 framer intr_status 0xC1
01:04:23: DSL 0/0 framer intr_status 0xC4
```

- ◦ 2-wire mode line 0:

```
Router# debug xdsl driver
xDSL driver debugging is on
00:58:22: DSL 0/0  dsp interrupt-download next block for line-0
00:58:23: DSL 0/0 framer intr_status 0xC0
00:58:24: DSL 0/0  dsp interrupt-download next block for line-0
00:58:24: DSL 0/0 framer intr_status 0xC0
00:58:37: DSL 0/0  dsp interrupt-download next block for line-0
00:58:37: DSL 0/0 framer intr_status 0xC0
00:58:38: DSL 0/0  dsp interrupt-download next block for line-0
00:58:38: DSL 0/0 framer intr_status 0xC0
00:58:38: DSL 0/0  dsp interrupt-download next block for line-0
00:58:38: DSL 0/0 DSP interrupt disabled
00:58:38: DSL 0/0  Download completed for line-0
00:58:38: DSL 0/0 Framer interrupt enabled
00:58:38: DSL 0/0 framer intr_status 0xC0
00:58:38:  DSL 0/0 controller Link up! line rate: 1600 Kbps
00:58:38: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:58:38:  Dslsar data rate 1600
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC1
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC4
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:58:38: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:58:38: DSL 0/0 framer intr_status 0xC1
00:58:38: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
```

- ◦ 2-wire mode line 1:

```
Router# debug xdsl driver
xDSL driver debugging is on
00:55:15: DSL 0/0  dsp interrupt-download next block for line-1
00:55:15: DSL 0/0 framer intr_status 0xC0
00:55:16: DSL 0/0  dsp interrupt-download next block for line-1
00:55:16: DSL 0/0 framer intr_status 0xC0
00:55:17: DSL 0/0  dsp interrupt-download next block for line-1
00:55:17: DSL 0/0 framer intr_status 0xC0
```

```
00:55:19: DSL 0/0  dsp interrupt-download next block for line-1
00:55:19: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32: DSL 0/0  dsp interrupt-download next block for line-1
00:55:32: DSL 0/0 DSP interrupt disabled
00:55:32: DSL 0/0  Download completed for line-1
00:55:32: DSL 0/0 Framer interrupt enabled
00:55:32: DSL 0/0 framer intr_status 0xC0
00:55:32:  DSL 0/0 controller Link up! line rate: 1600 Kbps
00:55:32: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:55:32:  Dslsar data rate 1600
00:55:46: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
00:55:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed state to up
00:56:28: DSL 0/0 framer intr_status 0xC8
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:28: DSL 0/0 framer intr_status 0xC8
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:28: DSL 0/0 framer intr_status 0xC2
00:56:28: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:28: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC8
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC2
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0
00:56:33: DSL 0/0 framer intr_status 0xC8  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
00:56:33: DSL 0/0  xdsl_gsi_int_disable(false):: 0x1
00:56:33: DSL 0/0 framer intr_status 0xC8
00:56:33: DSL 0/0  xdsl_gsi_int_disable(true):: 0x0
```

- **debug xdsl eoc** --Displays what is in the embedded operations channel messages. The following example shows the use of the **debug xdsl eoc** command and sample output.

```
Router# debug xdsl eoc

*Jan  3 18:34:46.824: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
*Jan  3 18:34:46.924: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:46.924: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:46.924: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:46.924: DSL 0/0: GT_FAIL
*Jan  3 18:34:46.924:   eoc_get_message for line::0
*Jan  3 18:34:46.924:  Rx EOC remove transparency:: 1F 1  0  46 10
*Jan  3 18:34:46.928: data_transparency_remove: Done, eoc packet size = 5

*Jan  3 18:34:46.928:   Good eoc packet received
*Jan  3 18:34:46.928:  incoming request eocmsgid: 1 from line 0
*Jan  3 18:34:46.928:  Tx Converted EOC message:: 21 81 1  43 43 49 53 43 4F 0  0  0  2
1  0  E9 61
*Jan  3 18:34:46.932: data_transparency_add: eoc packet size - before 17, after 17

*Jan  3 18:34:47.020: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:47.020: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:47.020: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:47.020: DSL 0/0: GT_FAIL
*Jan  3 18:34:47.020:   eoc_get_message for line::0
*Jan  3 18:34:47.020:  Rx EOC remove transparency:: 12 2  74 8A
*Jan  3 18:34:47.024: data_transparency_remove: Done, eoc packet size = 4

*Jan  3 18:34:47.024:   Good eoc packet received
*Jan  3 18:34:47.024:  incoming request eocmsgid: 2 from line 0
*Jan  3 18:34:47.024:  Tx Converted EOC message:: 21 82 1  0  0  0  0  0  52 33 2E 30 2E
31 43 4E 53 38 44 44 30 41 41 41 43 43 49 53 43 4F 0  0  0  57 49 43 2D 53 48 44 53 4C 2D
56 32 46 4F 43 30 38 33 37 35 55 41 4C 0  31 32 2E 34 28 33 2E 35 2E 31 29 0  66 74
*Jan  3 18:34:47.044: data_transparency_add: eoc packet size - before 71, after 71
```

```
*Jan  3 18:34:47.116: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:47.116: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:47.116: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:47.116: DSL 0/0: GT_FAIL
*Jan  3 18:34:47.116:   eoc_get_message for line::0
*Jan  3 18:34:47.116:  Rx EOC remove transparency:: 12 3  0  0  6D E9
*Jan  3 18:34:47.120: data_transparency_remove: Done, eoc packet size = 6

*Jan  3 18:34:47.120:   Good eoc packet received
*Jan  3 18:34:47.120:  incoming request eocmsgid: 3 from line 0
*Jan  3 18:34:47.120:  Tx Converted EOC message:: 21 83 0  0  0  1  AC
*Jan  3 18:34:47.120: data_transparency_add: eoc packet size - before 7, after 7
GSI Tx buffer yet to transmit

*Jan  3 18:34:47.212: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:47.212: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:47.212: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:47.212: DSL 0/0: GT_FAIL
*Jan  3 18:34:47.212:   eoc_get_message for line::0
*Jan  3 18:34:47.212:  Rx EOC remove transparency:: 12 5  0  0  0  E9 0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  32 42
*Jan  3 18:34:47.216: data_transparency_remove: Done, eoc packet size = 24

*Jan  3 18:34:47.216:   Good eoc packet received
*Jan  3 18:34:47.216:  incoming request eocmsgid: 5 from line 0
*Jan  3 18:34:47.220:  Tx Converted EOC message:: 21 85 0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  1E AB
*Jan  3 18:34:47.224: data_transparency_add: eoc packet size - before 26, after 26
GSI Tx buffer yet to transmit
GSI Tx buffer yet to transmit

*Jan  3 18:34:47.224: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:47.224: DSL 0/0: Current length 40 GTI_EOM
*Jan  3 18:34:47.224: DSL 0/0: GT_FAIL
*Jan  3 18:34:51.824: xdsl_background_process:
*Jan  3 18:34:51.824:  sending request eocmsgid: 12
*Jan  3 18:34:51.824:  Tx Converted EOC message:: 21 C  C0 FF
*Jan  3 18:34:51.824: data_transparency_add: eoc packet size - before 4, after 4

*Jan  3 18:34:51.824:  size of eoc full status request :: 2
*Jan  3 18:34:51.928: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:51.928: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:51.928: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:51.928: DSL 0/0: GT_FAIL
*Jan  3 18:34:51.928:   eoc_get_message for line::0
*Jan  3 18:34:51.928:  Rx EOC remove transparency:: 12 C  A  63
*Jan  3 18:34:51.932: data_transparency_remove: Done, eoc packet size = 4

*Jan  3 18:34:51.932:   Good eoc packet received
*Jan  3 18:34:51.932:  incoming request eocmsgid: 12 from line 0
*Jan  3 18:34:51.932:  Tx Converted EOC message:: 21 8C 0  F  D3 1  0  0  5  2  46 5  1
44 59
*Jan  3 18:34:51.932: data_transparency_add: eoc packet size - before 15, after 15

*Jan  3 18:34:51.936:  size of eoc status response :: 13
*Jan  3 18:34:51.936:  Tx Converted EOC message:: 21 8C 0  10 D3 1  0  0  6  1  46 5  2
50 2C
*Jan  3 18:34:51.936: data_transparency_add: eoc packet size - before 15, after 15

*Jan  3 18:34:51.936:  size of eoc status response :: 13
*Jan  3 18:34:51.940:  Tx Converted EOC message:: 21 89 4  DB 82
*Jan  3 18:34:51.940: data_transparency_add: eoc packet size - before 5, after 5

*Jan  3 18:34:51.940:  size of eoc status response :: 3GSI Tx buffer yet to transmit
GSI Tx buffer yet to transmit

*Jan  3 18:34:52.024: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:52.024: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:52.024: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:52.024: DSL 0/0: GT_FAIL
*Jan  3 18:34:52.024:   eoc_get_message for line::0
*Jan  3 18:34:52.024:  Rx EOC remove transparency:: 12 11 6E A8
*Jan  3 18:34:52.024: data_transparency_remove: Done, eoc packet size = 4
```

```
*Jan  3 18:34:52.028:   Good eoc packet received
*Jan  3 18:34:52.028:  incoming request eocmsgid: 17 from line 0
*Jan  3 18:34:52.028:  Tx Converted EOC message:: 21 91 0  0  0  D6 56
*Jan  3 18:34:52.028: data_transparency_add: eoc packet size - before 7, after 7

*Jan  3 18:34:52.028:  size of eoc status response :: 5GSI Tx buffer yet to transmit
GSI Tx buffer yet to transmit

*Jan  3 18:34:52.120: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:52.120: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:52.120: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:52.120: DSL 0/0: GT_FAIL
*Jan  3 18:34:52.120:   eoc_get_message for line::0
*Jan  3 18:34:52.120:  Rx EOC remove transparency:: 12 8C 0  3  0  B  7  5  D8 4  5F 6
1  27 64
*Jan  3 18:34:52.124: data_transparency_remove: Done, eoc packet size = 15

*Jan  3 18:34:52.124:   Good eoc packet received
*Jan  3 18:34:52.216: DSL 0/0: line 0 EOC Rcv  Intr :: 0x4
*Jan  3 18:34:52.216: DSL 0/0:Current length 40 GTI_OK
*Jan  3 18:34:52.216: DSL 0/0:msg rcvd line 0
*Jan  3 18:34:52.216: DSL 0/0: GT_FAIL
*Jan  3 18:34:52.216:   eoc_get_message for line::0
*Jan  3 18:34:52.216:  Rx EOC remove transparency:: 12 8C 0  5  0  3  0  0  12 3  2  26
2  1C 4F
*Jan  3 18:34:52.220: data_transparency_remove: Done, eoc packet size = 15
```

- **debug xdsl error** --Displays error messages. The following example shows the **debug xdsl error**command.

```
Router# debug xdsl error

xDSL error debugging is on
Router#
```

Configuration Examples for ATM Mode for Two-Wire or Four-Wire SHDSL

Router A CPE Configuration Example

```
controller DSL 1/2
 mode atm
 line-term cpe
 line-mode 2-wire line-zero
 dsl-mode shdsl symmetric annex B
!
!
!
!
connect hp DSL 1/0 0 DSL 1/2 0
!
!
```

Router B CO Configuration Example

```
Current configuration : 3183 bytes
```

```
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3725
!
boot-start-marker
boot system flash c3725-is-mz.0424
boot system tftp shriv/c3725-is-mz.new 223.255.254.254
boot-end-marker
!
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
!
!
!
controller DSL 0/0
 mode atm
 line-term co
 line-mode 4-wire enhanced
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 0/1
 mode atm
 line-term co
 line-mode 4-wire enhanced
 dsl-mode shdsl symmetric annex B
 line-rate 4608
controller DSL 0/2
 mode atm
 line-term co
 line-mode 4-wire enhanced
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
controller DSL 1/0
 mode atm
 line-term co
 line-mode 4-wire enhanced
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
!
!
interface ATM0/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/0.1 point-to-point
 ip address 5.0.0.1 255.0.0.0
 pvc 2/100
  vbr-rt 2000 2000
  oam-pvc 0
  encapsulation aal5mux ip
```

```
 !
!
interface FastEthernet0/0
 ip address 1.3.208.25 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface ATM0/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM0/1.1 point-to-point
 ip address 6.0.0.1 255.0.0.0
 pvc 2/100
  cbr 4608
 !
!
interface FastEthernet0/1
 mac-address 0000.0000.0011
 ip address 70.0.0.2 255.0.0.0 secondary
 ip address 90.0.0.2 255.0.0.0 secondary
 ip address 50.0.0.2 255.0.0.0
 load-interval 30
 speed 100
 full-duplex
 no cdp enable
!
interface ATM0/2
 no ip address
 no atm ilmi-keepalive
 clock rate aal5 8000000
!
interface ATM0/2.1 point-to-point
 ip address 7.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4200
 !
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 clock rate aal5 5300000
!
interface ATM1/0.1 point-to-point
 ip address 8.0.0.1 255.0.0.0
 pvc 2/100
  vbr-nrt 4608 4608
 !
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 172.19.163.44
ip classless
ip route 60.0.0.0 255.0.0.0 ATM1/0.1
ip route 80.0.0.0 255.0.0.0 ATM0/1.1
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0
ip route 223.255.254.254 255.255.255.255 1.3.0.1
```

```
ip http server
!
!
access-list 101 permit ip host 20.0.0.2 host 20.0.0.1
snmp-server community public RO
snmp-server enable traps tty
no cdp run
!
!
!
control-plane
!
!
!
!
!
!
!
alias exec c conf t
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
end
```

Additional References

For additional information related to the ATM Mode for Two-Wire or Four-Wire SHDSL feature, refer to the following references.

Related Documents

Related Topic	Document Title
1-port G.SHDSL WAN interface card	1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers, Release 12.2(8)T
Voice configuration	Cisco IOS Voice Configuration Library, Release 12.3
Voice commands	*Cisco IOS Voice Command Reference*, Release 12.3
IP configuration	*Cisco IOS IP Configuration Guide* , Release 12.3
ATM configuration	"Configuring ATM" in the *Wide-Area Networking Configuration Guide*, Release 12.3
Voice over ATM with AAL5 and AAL2 support	Voice over ATM, Release 12.3

Standards

Standards	Title
ITU-T G.991.2 (SHDSL)	Single-Pair High-Speed Digital Subscriber Line (SHDSL) Transceivers
ITU-T G.994.1 (G.HDSL)	Handshake Procedures for Digital Subscriber Line (DSL) Transceivers

MIBs

MIBs	MIBs Link
• ATM MIB • HDSL2-SHDSL-LINE-MIB(RFC3276) • G.SHDSL MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for ATM Mode for Two-Wire or Four-Wire SHDSL

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

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

Table 34 Feature Information for ATM Mode for Two-Wire or Four-Wire SHDSL

Feature Name	Releases	Feature Information
ATM Mode for Two-Wire or Four-Wire SHDSL	12.3(4)XD 12.3(4)XG 12.3(7)T 12.3(4)XG1 12.3(11)T 12.3(14)T 12.4(2)XA 12.4(5)	In Cisco IOS Release 12.3(4)XD, this feature (WIC-1SHDSL-V2) was introduced on the Cisco 2600 series and Cisco 3700 series routers to add 4-wire support. 2-wire support was previously available in Cisco IOS Release 12.2(8)T. For more information, see the document "1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers". This feature (WIC-1SHDSL-V2) was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers. This feature (WIC-1SHDSL-V2) was integrated into the Cisco IOS Release 12.3(7)T on the Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers. Cisco 1700 series routers do not support the WIC-1SHDSL-V2 in this release. In Cisco IOS Release 12.3(4)XG1, support for the auto line-mode feature was added. In Cisco IOS Release 12.3(11)T, support for the following was added: additional annex parameters for Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3631, Cisco 3700, and Cisco 3800 series routers; the HDSL2-SHDSL-LINE-MIB (RFC3276); and support for the ATM Mode for SHDSL feature was added for Cisco 2800 series and Cisco 3800 series routers. In Cisco IOS Release 12.3(14)T, support was added for Cisco 1800 series routers and the Cisco 2801 integrated services router.

Feature Name	Releases	Feature Information
		In Cisco IOS Release 12.4(2)XA, support was added for the WIC-1SHDSL-V3 interface card. Support for the WIC-1SHDSL-V3 interface card was integrated into the Cisco IOS Release 12.4(5) The following commands were introduced or modified: **controller dsl**, **dsl-mode shdsl symmetric annex**, **ignore-error-duration**, **line-mode**, **line-rate**, **line-term**, **loopback (DSL controller)**, **show controller dsl**, **snr margin**, **debug xdsl application**, **debug xdsl driver**, **debug xdsl eoc**, **debug xdsl error**.

Glossary

ABR--available bit rate. An ATM service type in which the ATM network makes a "best effort" to meet the transmitter's bandwidth requirements. ABR uses a congestion feedback mechanism that allows the ATM network to notify the transmitters that they should reduce their rate of data transmission until the congestion decreases. Thus, ABR offers a qualitative guarantee that the transmitter's data can get to the intended receivers without unwanted cell loss.

ATM--Asynchronous Transfer Mode. A form of digitized data transmission based on fixed-length cells that can carry data, voice, and video at high speeds.

CBR--constant bit rate. A data transmission that can be represented by a nonvarying, or continuous, stream of bits or cell payloads. Applications such as voice circuits generate CBR traffic patterns. CBR is an ATM service type in which the ATM network guarantees to meet the transmitter's bandwidth and quality-of-service (QoS) requirements.

CO--central office. Local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occur.

CPE--customer premises equipment. CPE includes devices, such as CSU/DSUs, modems, and ISDN terminal adapters, required to provide an electromagnetic termination for wide-area network circuits before connecting to the router or access server. This equipment was historically provided by the telephone company, but is now typically provided by the customer in North American markets.

Downstream--Refers to the transmission of data from the central office (CO or COE) to the customer premises equipment (CPE).

G.SHDSL--Multirate Symmetrical High-Speed Digital Subscriber Line.

UBR--unspecified bit rate. QoS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network, but there are no guarantees in terms of cell loss rate and delay. Compare with ABR (available bit rate), CBR, and VBR.

Upstream--Refers to the transmission of data from the customer premises equipment (CPE) to the central office equipment (CO or COE).

VBR--variable bit rate. QOS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (rt) class and non-real time (nrt) class.

VBR-rt--VBR-real-time is used for connections in which there is a fixed timing relationship between samples.

VBR-nrt--VBR-non-real-time is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.

1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers

This document describes the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card (WIC) (WIC-1SHDSL) on Cisco 2600 series and Cisco 3600 series routers in Cisco IOS Release 12.2(8)T.

G.SHDSL is an ATM-based, multirate, high-speed (up to 2.3 MB), symmetrical digital subscriber line technology for data transfer between a single customer premises equipment (CPE) subscriber and a central office.

G.SHDSL is supported on the G.SHDSL WAN interface card (WIC-1SHDSL), a 1-port WAN interface card (WIC) for Cisco 2600 series and Cisco 3600 series routers.

The G.SHDSL WIC is compatible with the Cisco 6015, Cisco 6130, Cisco 6160, and Cisco 6260 Digital Subscriber Line Access Multiplexers (DSLAMs). The DSLAM must be equipped with G.SHDSL line cards that are compatible with the DSL service to be configured.

The G.SHDSL WIC supports ATM Adaptation Layer 2 (AAL2), ATM Adaptation Layer 5 (AAL5), and various classes of service for ATM

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for 1-Port G.SHDSL WAN Interface Card

A G.SHDSL WIC must be installed in the router to match the DSL service to be configured. A compatible G.SHDSL line card must be installed in the DSLAM.

Restrictions for 1-Port G.SHDSL WAN Interface Card

- The G.SHDSL WIC does not support dual latency. When the DSL link is intended to support both voice and data traffic simultaneously, the total supported data rate must be reduced to adjust for the reduced coding gain, which is usually present with high-latency traffic.
- The G.SHDSL WIC does not support Dying Gasp in ANSI T1.413 Issue 2.
- The G.SHDSL WIC does not support available bit rate (ABR) class of service (CoS).
- The G.SHDSL WIC should be inserted only into onboard WIC slots or 1FE2W, 2W, 1FE1R, 2FE2W network modules. This WIC is not supported in old combination network modules.

Information About 1-Port G.SHDSL WAN Interface Card

- Benefits, page 436

Benefits

- Enables business-class broadband service with voice integration, scalable performance, flexibility, and security.
- Symmetrical WAN speeds (up to 2.3Mbps) over a single copper pair.
- Repeatable and has thirty percent longer reach than SDSL.
- Rate adaptive with G.HS "handshake" Protocol.
- Based on ITU Recommendation G.991.2 (Accepted Worldwide).
- Support for G.SHDSL Annex A (U.S. signaling) and Annex B (European signaling).
- Multiple G.SHDSL WAN Interface Cards configurable per Cisco 2600 series and Cisco 3600 series chassis.
- Toll-quality voice over IP delivery over AAL2 and AAL5.
- Provides ATM traffic management to enable service providers to manage their core ATM network infrastructures.
- Supports ATM class of service features constant bit rate (CBR), variable bit rate-nonreal time (VBR-nrt), variable bit rate-real time (VBR-rt), and unspecified bit rate (UBR and UBR+).
- Operates back-to-back or through a DSLAM.
- Sustains up to 23 virtual circuits per WAN on a WIC in Cisco 2600 series and Cisco 3600 series routers.

How to Configure 1-Port G.SHDSL WAN Interface Card

- Configuring G.SHDSL on a Cisco Router, page 437

- Configuring ILMI on the DSLAM Connected to the G.SHDSL WIC, page 440
- Verifying ATM Configuration, page 440

Configuring G.SHDSL on a Cisco Router

To configure G.SHDSL service on a Cisco router containing a G.SHDSL WIC, complete the following steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface atm 1/0**
2. **ip address** *IP-address*
3. **atm ilmi-keepalive** *seconds*
4. **pvc** [*name*] *vpi/vci*
5. **protocol ip** *IP-address*
6. **vbr-rt** *peak-rate average-rate burst*
7. **encapsulation aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap**
8. **exit**
9. **dsl operating-mode gshdsl symmetric annex** {**A**| **B**} }
10. **equipment-type co** | **cpe**
11. **dsl linerate** *kbps* | **auto**
12. **exit**
13. **exit**
14. **show interface atm 1/0**
15. **clear interface atm 1/0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface atm 1/0** **Example:** `Router(config)# interface atm 1/0`	Enters ATM configuration mode for interface ATM 0 in slot 1. **Note** If a slot has two subslots for WIC modules and no ATM interface is present in subslot 0, the WIC will take ATM x/0 as its interface number even if placed in subslot 1 (ATMx/1). If a two-port ATM module is present in subslot 0, the WIC will use ATM x/2 as its interface number. This subslot number is pertinent to all interface commands such as **show interface atm** and **show dsl interface atm**.
Step 2	**ip address** *IP-address* **Example:** `Router(config-if)# ip address 10.3.0.1 255.255.255.0`	Assigns an IP address to the DSL ATM interface.

	Command or Action	Purpose
Step 3	**atm ilmi-keepalive** *seconds* **Example:** `Router(config-if)# atm ilmi-keepalive 10`	(Optional) Enables Integrated Local Management Interface (ILMI) keepalives. If you enable ILMI keepalives without specifying the seconds, the default time interval is 3 seconds.
Step 4	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if-vc)# pvc 10/100`	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM permanent virtual circuit (PVC) by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is an unspecified bit rate (UBR); the default encapsulation is AAL5+LLC/SNAP.
Step 5	**protocol ip** *IP-address* **Example:** `Router(config-if-vc)# protocol ip 10.3.0.2 broadcast`	(Optional) Enables IP connectivity and create a point-to-point IP address for the virtual circuit (VC).
Step 6	**vbr-rt** *peak-rate average-rate burst* **Example:** `Router(config-if-vc)# vbr-rt 672 672 512`	(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping. • *Peak rate* --Peak information rate (PIR) • *Average rate* --Average information rate (AIR) • *Burst* --Burst size in cells
Step 7	**encapsulation aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap** **Example:** `Router(config-if-vc)# encapsulation aal2`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • **aal1** --AAL1 • **aal2** --AAL2 • **aal5ciscoppp** --Cisco PPP over AAL5 • **aal5mux** --AAL5+MUX • **aal5nlpid** --AAL5+NLPID • **aal5snap** --AAL5+LLC/SNAP The default is **aal5snap**.
Step 8	**exit** **Example:** `Router(config-if-vc)# exit`	Exits from interface-atm-vc configuration mode.

	Command or Action	Purpose
Step 9	**dsl operating-mode gshdsl symmetric annex** {**A**| **B**} } **Example:** `Router(config-if)# dsl operating-mode gshdsl symmetric annex A`	Configures the DSL interface to operate in a specified DSL mode: • **gshdsl** --Configures multirate, high-speed DSL per ITU G.991.2 • **symmetric** --Configures symmetrical mode per ITU G.992.1. • **annex** --Configures the regional operating parameters. • **A** --Sets the operating parameters for North America. This value is the default. • **B** --Sets the operating parameters for Europe. The default is **g shdsl symmetric annex A**.
Step 10	**equipment-type co** | **cpe** **Example:** `Router(config-if)# equipment-type cpe`	Configures the DSL interface to function as central office equipment or customer premises equipment: • **co** --The WIC functions as central office equipment and can interface with another G.SHDSL WIC configured as **cpe**. • **cpe** --The WIC functions as customer premises equipment and can interface with a DSLAM or with another G.SHDSL WIC configured as **co**. The default is **cpe**.
Step 11	**dsl linerate** *kbps* | **auto** **Example:** `Router(config-if)# dsl linerate 264`	Configures the DSL line rate: • *kbps* --Line rate (data transfer rate) in kilobits per second. Allowable entries are **72**, **136**, **200**, **264**, **392**, **520**, **776**, **1032**, **1160**, **1544**, **2056**, and **2312**. • **auto** --The WIC automatically trains for an optimal line rate by negotiating with the far-end DSLAM or WIC. The default is **auto**.
Step 12	**exit** **Example:** `Router(config-if)# exit`	Exits from ATM interface configuration mode.
Step 13	**exit** **Example:** `Router(config)# exit`	Exits from global configuration mode.
Step 14	**show interface atm 1/0** **Example:** `Router# show interface atm 1/0`	Verifies the ATM interface configuration.

	Command or Action	Purpose
Step 15	**clear interface atm 1/0** **Example:** `Router# clear interface atm 1/0`	Permits the configuration changes to take effect.

Configuring ILMI on the DSLAM Connected to the G.SHDSL WIC

The ILMI protocol allows DSLAMs to be used for ATM address registration across an ATM User-Network Interface (UNI). If ILMI is configured on the G.SHDSL WIC, the ATM PVC must be configured on the DSLAM. All switch terminating connections use interface 0/0 to connect to the switch CPU.

For information about configuring the DSLAM, see the Configuration Guide for Cisco DSLAMs with NI-2.

Verifying ATM Configuration

Use the following commands to verify your configuration:

- To verify current configuration and to view the status for all controllers, use the **show running-config** command.
- To view ATM controller statistics, use the **show controllers atm** *slot/port*command.
- To verify the PVC status, use the **show atm vc** command. Make sure that active PVCs are up.
- To help identify ATM related events as they are generated, use the **debug atm events** command.
- To indicate which interfaces are having trouble, use the **debug atm errors** command.
- To identify an entry for the ATM interface you configured and to show an entry for the ATM slot/port you configured, use the **show ip route** command.
- To view the status of ATM interface, use the **show interface atm**command. Make sure that the ATM slot/port and the line protocol are up, as shown in the following example:

```
Router# show interface
 atm 1/0

ATM1/0 is up, line protocol is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 800 Kbit, DLY 2560 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5 AAL2, PVC mode
  24 maximum active VCs, 256 VCs per VP, 2 current VCCs
  VC idle disconnect time:300 seconds
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters 03:16:00
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2527 packets input, 57116 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10798 packets output, 892801 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

```
Router# show atm vc
            VCD /                                    Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
1/0.3      2            9    36   PVC    MUX      UBR     800                UP
1/0.2      1            9    37   PVC    SNAP     UBR     800                UP
Router# show controllers
 atm 1/0

Interface ATM1/0 is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
IDB:    62586758  Instance:6258E054  reg_dslsar:3C810000  wic_regs:3C810080
PHY Inst:62588490  Ser0Inst:62573074  Ser1Inst: 6257CBD8  us_bwidth:800
Slot:   1         Unit:    1         Subunit:  0         pkt Size:4496
VCperVP:256       max_vp:  256       max_vc:   65536     total vc:2
rct_size:65536     vpivcibit:16       connTblVCI:8         vpi_bits:8
vpvc_sel:3         enabled: 0        throttled:0
WIC    Register   Value      Notes
---------------   ---------- ----------
FPGA Dev ID (LB)  0x44       'D'
FPGA Dev ID (UB)  0x53       'S'
FPGA Revision     0x99
WIC Config Reg    0x45       WIC / VIC select = WIC;
                             CTRLE addr bit 8 = 1;
                             OK LED on;
                             LOOPBACK LED off;
                             CD LED on;
WIC Config Reg2   0x07       Gen bus error on bad ADSL access
Int 0 Enable Reg  0x03       ADSL normal interrupt enabled
                             ADSL error interrupt enabled
```

- To view the status of the G.SHDSL modem, use the **show dsl interface atm** command. If the line is down, the following statement appears: Line is not active. Some of the values may not be accurate. You can also verify whether the equipment type and operating mode configuration are correct for your application.

Sample output--The WIC is configured as central office equipment, and the line is up

```
Router# show dsl interface atm 0/0

Globespan G.SHDSL Chipset Information
 Equipment Type:        Central Office
 Operating Mode:        G.SHDSL
 Clock Rate Mode:       Auto rate selection Mode
 Reset Count:           2
 Actual rate:           2320 Kbps
 Modem Status:          Data
 Noise Margin:          43 dB
 Loop Attenuation:      0.0 dB
 Transmit Power:        13.5 dB
 Receiver Gain:         204.8000 dB
 Last Activation Status:No Failure
 CRC Errors:            0
 Chipset Version:       1
 Firmware Version:      R1.0
 Farend Statistics since CO boot-time:
    CRC Errors:      0
    Errored Seconds: 0
    Severly ES:      0
    Un Available S:  48
    Loss Of Sync S:  0
```

Sample output--The WIC is configured as customer premises equipment, and the line is up

```
Router# show dsl interface atm 0/0

Globespan G.SHDSL Chipset Information
 Equipment Type:        Customer Premise
 Operating Mode:        G.SHDSL
 Clock Rate Mode:       Auto rate selection Mode
```

```
 Reset Count:           1
 Actual rate:           2320 Kbps
 Modem Status:          Data
 Noise Margin:          42 dB
 Loop Attenuation:      0.0 dB
 Transmit Power:        13.5 dB
 Receiver Gain:         204.8000 dB
 Last Activation Status:No Failure
 CRC Errors:            0
 Chipset Version:       1
 Firmware Version:      R1.0
```

Configuration Examples for 1-Port G.SHDSL WAN Interface Card

Configuration in CPE Mode Example

The following example shows a G.SHDSL configuration of VoATM over AAL2, operating in customer premises equipment (CPE) mode, on a Cisco 2600 series router. This router in CPE mode can be linked to either a DSLAM or to another router that is configured to operate in central office (CO) mode.

```
Router#
Router# show running config
Building configuration...
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host1
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
ip host host2 225.255.255.224
!
no mgcp timer receive-rtcp
call rsvp-sync
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1 type e&m-wink-start
 ds0-group 1 timeslots 2 type e&m-wink-start
.
.
.
ds0-group 23 timeslots 24 type e&m-wink-start
!
controller T1 1/1
 framing esf
 linecode b8zs
!
interface Ethernet0/0
 ip address 209.165.202.128 255.255.255.224
 half-duplex
 no cdp enable
!
```

```
interface Serial0/0
 no ip address
 shutdown
!
interface ATM0/1
 ip address 209.165.201.1 255.255.255.224
 dsl operating-mode gshdsl symmetric annex A
 dsl equipment-type cpe
 dsl linerate auto
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 pvc 10/100
  vbr-rt 672 672 512
  encapsulation aal2
 !
 pvc 10/200
  protocol ip 209.165.202.159 broadcast
  encapsulation aal5snap
 !
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 209.165.202.128 255.255.255.224 Ethernet0/0
no ip http server
!
!
snmp-server engineID local 000000090200003080477F20
snmp-server manager
!
voice-port 1/0:0
 local-alerting
 timeouts wait-release 3
 connection trunk 3001
!
voice-port 1/0:1
 local-alerting
 timeouts wait-release 3
 connection trunk 3002
.
.
.
voice-port 1/0:23
 local-alerting
 timeouts wait-release 3
 connection trunk 3024
 shutdown
!
dial-peer cor custom
!
dial-peer voice 3001 voatm
 destination-pattern 3001
 called-number 4001
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 31
 codec aal2-profile ITUT 1 g711ulaw
 no vad
!
dial-peer voice 3002 voatm
 destination-pattern 3002
 called-number 4002
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 32
 codec aal2-profile custom 100 g726r32
 no vad
!
dial-peer voice 3003 voatm
 destination-pattern 3003
 called-number 4003
```

```
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 33
 codec aal2-profile ITUT 7 g729abr8
 no vad
.
.
.
dial-peer voice 3024 voatm
 destination-pattern 3024
 called-number 3024
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 54
 codec aal2-profile ITUT 7 g729abr8
 no vad
!
dial-peer voice 1 pots
 destination-pattern 4001
 port 1/0:0
!
dial-peer voice 2 pots
 destination-pattern 4002
 port 1/0:1
.
.
.
dial-peer voice 24 pots
 destination-pattern 4024
 port 1/0:23
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
no scheduler allocate
end
```

Configuration in CO Mode Example

The following example shows a G.SHDSL configuration of VoATM over AAL2, operating in central office (CO) mode, on a Cisco 2600 series router. This router in CO mode can be linked to another router that is configured to operate in CPE mode.

```
Router#
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname host2
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
ip host host2 225.255.255.224
!
no mgcp timer receive-rtcp
call rsvp-sync
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1 type e&m-wink-start
 ds0-group 1 timeslots 2 type e&m-wink-start
.
```

```
.
.
ds0-group 23 timeslots 24 type e&m-wink-start
!
controller T1 1/1
 framing esf
 linecode b8zs
!
interface Ethernet0/0
 ip address 209.165.202.128 255.255.255.224
 half-duplex
 no cdp enable
!
interface Serial0/0
 no ip address
 shutdown
!
interface ATM0/1
 ip address 209.165.201.1 255.255.255.224
 dsl operating-mode gshdsl symmetric annex A
 dsl equipment-type co
 dsl linerate auto
 load-interval 30
 atm vc-per-vp 256
 no atm ilmi-keepalive
 pvc 10/100
  vbr-rt 672 672 512
  encapsulation aal2
 !
 pvc 10/200
  protocol ip 209.165.202.159 broadcast
  encapsulation aal5snap
 !
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 209.165.202.128 255.255.255.224 Ethernet0/0
no ip http server
!
!
snmp-server engineID local 000000090200003080477F20
snmp-server manager
!
voice-port 1/0:0
 local-alerting
 timeouts wait-release 3
 connection trunk 3001
!
voice-port 1/0:1
 local-alerting
 timeouts wait-release 3
 connection trunk 3002
.
.
.
voice-port 1/0:23
 local-alerting
 timeouts wait-release 3
 connection trunk 3024
 shutdown
!
dial-peer cor custom
!
dial-peer voice 3001 voatm
 destination-pattern 3001
 called-number 4001
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 31
 codec aal2-profile ITUT 1 g711ulaw
```

```
 no vad
!
dial-peer voice 3002 voatm
 destination-pattern 3002
 called-number 4002
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 32
 codec aal2-profile custom 100 g726r32
 no vad
!
dial-peer voice 3003 voatm
 destination-pattern 3003
 called-number 4003
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 33
 codec aal2-profile ITUT 7 g729abr8
 no vad
.
.
.
dial-peer voice 3024 voatm
 destination-pattern 3024
 called-number 3024
 session protocol aal2-trunk
 session target ATM0/1 pvc 10/100 54
 codec aal2-profile ITUT 7 g729abr8
 no vad
!
dial-peer voice 1 pots
 destination-pattern 4001
 port 1/0:0
!
dial-peer voice 2 pots
 destination-pattern 4002
 port 1/0:1
.
.
.
dial-peer voice 24 pots
 destination-pattern 4024
 port 1/0:23
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
no scheduler allocate
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Voice configuration	• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*
Configuring IP	*Cisco IOS IP Configuration Guide*.
Configuring ATM	*Configuring ATM* in the*Wide-Area Networking Configuration Guide*
Installing Cisco 2600 series hardware	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/index.htm
Installing Cisco 3600 series hardware	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm

Standards

Standard	Title
ITU-T G.991.2	*SHDSL*

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

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 1-Port G.SHDSL WAN Interface Card

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 35 Feature Information for 1-Port G.SHDSL WAN Interface Card

Feature Name	Releases	Feature Information
1-Port G.SHDSL WAN Interface Card	12.2(4)XL 12.2(8)T	The Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card (WIC) (WIC-1SHDSL) on Cisco 2600 series and Cisco 3600 series routers in Cisco IOS Release 12.2(8)T. This feature is supported on the following platforms: Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2621, Cisco 2650, Cisco 2651, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3661, Cisco 3662 The following commands were introduced or modified: **dsl equipment-type**, **dsl linerate**, **dsl operating-mode (G.SHDSL)**.

Glossary

ABR--available bit rate.

ADSL--asymmetric digital subscriber line. Available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

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

CLI--command-line interface.

CO--central office. Local exchange (local switch) that terminates individual local telephone subscriber lines for switching, and connects to the public network. A CO is known as a class 5 switch office. For example, 5ESS by Lucent and DMS 100 by Nortel.

CPE--customer premise equipment. Devices such as channel service units (CSUs)/data service units (DSUs), modems, and ISDN terminal adapters, required to provide an electromagnetic termination for wide-area network circuits before connecting to the router or access server. This equipment was historically provided by the telephone company, but is now typically provided by the customer in North American markets.

DSL--digital subscriber line available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

FXO--foreign exchange office. An FXO interface connects to a central office.

FXS--foreign exchange station. An FXS interface connects directly to a standard telephone, supplying ring voltage, dial tone, and so on.

G.SHDSL--Multirate Symmetrical High-Speed Digital Subscriber Line

IAD--integrated access device. A CPE device used to combine services from various sources onto a common platform for transmission on a common transport span. Typically, an IAD combines various voice and data services such as circuit-based services like traditional POTS and packet-switched services such as frame relay or ATM.

PVC--permanent virtual circuit.

G.SHDSL Symmetric DSL Support for Cisco IAD2420 Series IAD

This document describes the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the Cisco IAD2420 series integrated access devices (IADs) in Cisco IOS Release 12.2(8)T.

G.SHDSL is ATM-based, multirate, high-speed (up to 2.3 MB), symmetrical digital subscriber line technology for data transfer between a single customer premises equipment (CPE) subscriber and a central office (CO). G.SHDSL refers to the approved standard officially designated in ITU-T G.991.2.

The Cisco IAD2420 series IADs support G.SHDSL in the following models: IAD2424-8FXS, IAD2424-16FXS, IAD2424-16FXS8FXO, and IAD2424-1T1. These models are compatible with the Cisco 6160 and Cisco 6260 Digital Subscriber Line Access Multiplexers (DSLAM). The DSLAM must be equipped with compatible G.SHDSL line cards.

The Cisco IAD2424 IAD supports ATM Adaption Layer 2 (AAL2), ATM Adaption Layer 5 (AAL5), and quality of service (QoS) features for both voice and data services.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for G.SHDSL Symmetric DSL Support

A compatible G.SHDSL line card must be installed in the DSLAM.

Restrictions for G.SHDSL Symmetric DSL Support

The wetting current function is not supported as part of G.SHDSL.

Information About G.SHDSL Symmetric DSL Support

- Benefits, page 452

Benefits

- Enables business class broadband service with voice integration, scalable performance, flexibility, and security.
- Aggregates G.SHDSL and other transport options into a single box.
- Provides G.SHDSL high-speed digital data transmissions between CPE and the CO.
- Supports AAL2 and AAL5 services and applications (including voice), ATM class of service (constant bit rate [CBR], variable bit rate-nonreal time [VBR-nrt], variable bit rate-real time [VBR-rt], and unspecified bit rate [UBR and UBR+]).
- Provides ATM traffic management and quality of service (QoS) features to enable service providers to manage their core ATM network infrastructures.

How to Configure G.SHDSL Symmetric DSL Support

- Configuring G.SHDSL on Cisco IAD2420 Series IADs, page 452
- Verifying ATM Configuration, page 456
- Verifying Your Configuration, page 457

Configuring G.SHDSL on Cisco IAD2420 Series IADs

To configure G.SHDSL service on the Cisco IAD2420 series IAD that supports G.SHDSL, complete the following steps, beginning in global configuration mode:

SUMMARY STEPS

1. **controller shdsl 0**
2. **mode atm**
3. **annex** {**a** | **b**
4. **line-rate auto** | *rate*
5. **exit**
6. **interface atm 0**
7. **ip address***Iip-address*
8. **atm ilmi-keepalive***seconds*
9. **pvc** [*name*] *vpi/vci*
10. **protocol ip***IP-address*
11. **vbr-rt***peak-rate average-rate burst*
12. **encapsulation aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap**
13. **exit**
14. **shutdown**
15. Router(config-if)# **no shutdown**
16. Router(config-if)# **exit**
17. Router(config)# **exit**
18. Router> **show interface atm 0**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller shdsl 0** **Example:** `Router(config)# controller shdsl 0`	Enters controller configuration mode and the controller number.
Step 2	**mode atm** **Example:** `Router(config-ctrl)# mode atm`	Enables ATM encapsulation and creates logical ATM interface 0. Controller framing is automatically set to Extended SuperFrame (ESF). The line code is automatically set to B8ZS.
Step 3	**annex** {**a** | **b** **Example:** `Router(config-ctrl)# annex a`	Specifies the regional operating parameters. Enter **a** for North America and **b** for Europe. The default is **a**.

	Command or Action	Purpose
Step 4	**line-rate auto** | *rate* **Example:** `Router(config-ctrl)# line-rate auto 1160`	Specifies the DSL line rate for the SHDSL port. The range is 192 to 2312 kbps. The default is **auto** (negotiated between the SHDSL port and the DSLAM). **Note** If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate. **Note** The maximum peak cell rate is 8 kbps less than the line rate.
Step 5	**exit** **Example:** `Router(config-ctrl)# exit`	Exits from controller configuration mode.
Step 6	**interface atm 0** **Example:** `Router(config)# interface atm 0`	Enters ATM configuration mode for interface ATM 0.
Step 7	**ip address***Iip-address* **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.255.0`	Assigns an IP address to the DSL ATM interface.
Step 8	**atm ilmi-keepalive***seconds* **Example:** `Router(config-if)# atm ilmi-keepalive 10`	(Optional) Enables Integrated Local Management Interface (ILMI) keepalives. If you enable ILMI keepalives without specifying the number of seconds, the default time interval is 3 seconds.
Step 9	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)# pvc 110/110`	Enters atm-virtual-circuit (interface-atm-vc) configuration mode, and configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers. The default traffic shaping is UBR; the default encapsulation is AAL5+LLC/SNAP.
Step 10	**protocol ip***IP-address* **Example:** `Router(config-if-vc)# protocol ip 10.1.0.2`	(Optional) Enables IP connectivity and creates a point-to-point IP address for the VC.

	Command or Action	Purpose
Step 11	**vbr-rt***peak-rate average-rate burst* **Example:** `Router(config-if-vc)# vbr-rt 2304 2304 65535`	(Optional) Configures the PVC for real-time variable bit rate (VBR) traffic shaping. • Peak rate = peak information rate (PIR) • Average rate = average information rate (AIR) • Burst = burst size in cells
Step 12	**encapsulation aal1** | **aal2** | **aal5ciscoppp** | **aal5mux** | **aal5nlpid** | **aal5snap** **Example:** `Router(config-if-vc)# encapsulation aal2`	(Optional) Configures the ATM adaptation layer (AAL) and encapsulation type. • Use the **aal2** keyword for AAL2 • Use the **aal5ciscoppp** keyword for Cisco PPP over AAL5 • Use the **aal5mux** keyword for AAL5+MUX • Use the **aal5nlpid** keyword for AAL5+NLPID • Use the **aal5snap** keyword for AAL5+LLC/SNAP (the default)
Step 13	**exit** **Example:** `Router(config-if-vc)# exit`	Exits from interface-ATM-VC configuration mode.
Step 14	**shutdown** **Example:** `Router(config-if)# shutdown`	Ensures that the ATM interface is shut down.
Step 15	Router(config-if)# **no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the ATM interface.
Step 16	Router(config-if)# **exit** **Example:** `Router(config-if)# exit` Exits from ATM interface configuration mode.	
Step 17	Router(config)# **exit** **Example:** `Router(config)# exit`	Exits from global configuration mode.

	Command or Action	Purpose
Step 18	Router> **show interface atm 0** **Example:** `Router> show interface atm 0`	Verifies the ATM interface configuration.

Verifying ATM Configuration

You can verify the ATM interface configuration by doing the following:

- To verify the ATM interface configuration, enter the **show interface atm 0**command in EXEC mode.

```
Router# show interface atm 0
ATM0 is up, line protocol is up
  Hardware is DSLSAR (with Globespan G.SHDSL Module)
  MTU 4470 bytes, sub MTU 4470, BW 800 Kbit, DLY 2560 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5 AAL2, PVC mode
  24 maximum active VCs, 256 VCs per VP, 2 current VCCs
  VC idle disconnect time:300 seconds
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters 03:16:00
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     2527 packets input, 57116 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10798 packets output, 892801 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

- For an SHDSL port, to verify the SHDSL controller status and view the statistics, enter the **show controller shdsl 0** command in EXEC mode.

```
Router# show controller shdsl 0
 SHDSL 0 controller UP
 SLOT 3: Globespan xDSL controller chipset
 Frame mode: Serial ATM
 Configured Line rate: 1160Kbps
 Line Re-activated 0 times after system bootup
 LOSW Defect alarm: None
 CRC per second alarm: None
 Line termination: CPE
 FPGA Revision: 9
        Current 15 min CRC: 0
        Current 15 min LOSW Defect: 0
        Current 15 min ES: 0
        Current 15 min SES: 0
        Current 15 min UAS: 7
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 7
 Chipset Version:  1
 Firmware Version:  R1.2
 Modem Status:  Data
 Line rate:  1160 Kbps
```

```
 Framer Sync Status: In Sync
 Rcv Clock Status: In the Range
 Loop Attenuation:  0.0 dB
 Transmit Power:  13.5 dB
 Receiver Gain:  11.420 dB
 SNR Sampling:  40
 Last Fail Mode:  No Failure
```

- To verify the SHDSL controller status and view the statistics, change state to administratively down and enter the **show controller shdsl 0** command in EXEC mode.

```
Router#
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
iad1(config)#contr shds 0
iad1(config-controller)#shut
iad1(config-controller)#
01:30:46: %CONTROLLER-5-UPDOWN: Controller SHDSL 0, changed state to administratively down
01:30:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0, changed state to down
iad1(config-controller)#end
Router# show controller shdsl 0
 SHDSL 0 controller ADMINDOWN
 SLOT 3: Globespan xDSL controller chipset
 Frame mode: Serial ATM
 Configured Line rate: 1160Kbps
 Line Re-activated 2 times after system bootup
 LOSW Defect alarm: None
 CRC per second alarm: None
 Line termination: CPE
 FPGA Revision: 9
        Current 15 min CRC: 0
        Current 15 min LOSW Defect: 0
        Current 15 min ES: 0
        Current 15 min SES: 0
        Current 15 min UAS: 7
        Previous 15 min CRC: 0
        Previous 15 min LOSW Defect: 0
        Previous 15 min ES: 0
        Previous 15 min SES: 0
        Previous 15 min UAS: 0
 Chipset Version:  1
 Firmware Version:  R1.2
 Modem Status:  Idle
```

Verifying Your Configuration

You can perform the following tests at any time to verify the hardware or software configuration of the Cisco IAD2420 series IADs:

- Display the hardware configuration with the **show version** command.
- Display T1 and SHDSL controllers with the **show controllers** command.
- Display the running configuration with the **show running-config** command

Display the configuration stored in NVRAM using the **show startup-config** command.

Configuration Examples for G.SHDSL Symmetric DSL Support

The following example shows a typical running configuration with the initial configuration tasks completed:

```
Router#
Router# show running config
Building configuration...
```

```
Current configuration : 1654 bytes
!
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot system flash:c2420-a2i8sv5-mz.1.0.9
logging rate-limit console 10 except errors
!
network-clock base-rate 56k
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
!
!
!
no voice confirmation-tone
voice-card 0
!
!
!
controller SHDSL 0
 mode atm
!
controller T1 1
 mode cas
 framing esf
 clock source loop-timed
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-immediate-start
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.0.0
!
interface Ethernet0
 ip address 1.3.95.50 255.255.0.0
 no ip mroute-cache
!
interface Serial0
 bandwidth 10000000
 ip address 180.100.9.11 255.255.255.0
 no keepalive
!
interface ATM0
 no ip address
 ip mroute-cache
 atm idle-cell-format itu
 atm enable-payload-scrambling
 no atm ilmi-keepalive
 pvc 110/110
  vbr-rt 2304 2304 65535
  vcci 2
  encapsulation aal2
 !
!
router eigrp 10
 network 10.0.0.0
 network 180.100.0.0
 no auto-summary
 no eigrp log-neighbor-changes
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 1.3.0.1
ip route 2.2.2.2 255.255.255.255 10.10.10.2
no ip http server
!
call rsvp-sync
!
voice-port 1:1
!
mgcp
mgcp call-agent 1.4.173.1 service-type mgcp version 0.1
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 1:1
!
!
line con 0
 exec-timeout 0 0
line aux 0
line 2 3
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Voice configuration	• *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2 • *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
Configuring IP	*Cisco IOS IP Configuration Guide*, Release 12.2.
Configuring ATM	"Configuring ATM" in the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2.
Configuring a DSLAM	*Configuration Guide for Cisco DSLAMs with NI-2*
Installing and configuring Cisco IAD2420 series IAD hardware and software	http://www.cisco.com/univercd/cc/td/doc/product/access/iad/iad2420/index.htm

Standards

Standard	Title
Supports ITU-T G.991.2	*SHDSL*

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for G.SHDSL Symmetric DSL 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 36 Feature Information for G.SHDSL Symmetric DSL Support

Feature Name	Releases	Feature Information
G.SHDSL Symmetric DSL Support	12.2(4)T3 12.2(8)T	In Cisco IOS Release 12.2(4)T3, the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature was supported on the G.SHDSL one-port WAN interface on the Cisco 2600 series and Cisco 3600 series routers. In Cisco IOS Release 12.2(8)T, the G.SHDSL feature was expanded to the Cisco IAD2420 series IADs. The following commands were introduced or modified: **controller shdsl 0**, **mode atm**, **show controller shdsl 0**.

Glossary

ADSL--Asymmetric DSL (ADSL) available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

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

CLI--command line interface.

CO--central office. Local exchange (local switch) that terminates individual local telephone subscriber lines for switching and connects to the public network. Known as a class 5 switch office. For example, 5ESS by Lucent and DMS 100 by Nortel.

CPE--customer premises equipment. Devices such as channel service units, data service units, modems, and ISDN terminal adapters, required to provide an electromagnetic termination for wide-area network circuits before connecting to the router or access server. This equipment was historically provided by the telephone company, but is now typically provided by the customer in North American markets.

DSL--Digital Subscriber Line available through several telecommunications carriers to accommodate the need for increased bandwidth for Internet access and telecommuting applications.

FXO--Foreign Exchange Office. An FXO interface connects to a central office.

FXS--Foreign Exchange Station: An FXS interface connects directly to a standard telephone, supplying ring voltage, dial tone, and so on.

G.SHDSL--Multirate Symmetrical High-Speed Digital Subscriber Line.

IAD--integrated access device. A CPE device used to combine services from various sources onto a common platform for transmission on a common transport span. Typically, an IAD combines various voice and data services such as circuit-based services like traditional telephone service and packet-switched services such as frame relay or ATM.

Monitoring and Retraining on Reception of Loss of Margin Messages

Loss of Margin (LoM) monitoring allows the router to handle asymmetric digital subscriber line (ADSL) loss of margin messages received from the digital subscriber line access multiplexer (DSLAM). The **dsl lom** command is used to set digital subscriber line (DSL) LoM monitoring. The **no dsl lom** command disables LoM monitoring after the router has been configured to monitor LoM messages.

When set to monitor LoM, the router will retrain with the DSLAM when it receives LoM messages consecutively for the number of times specified in the *number* argument.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About Monitoring and Retraining on Reception of Loss of Margin Messages

ATM Technology

Asynchronous Transfer Mode (ATM) is a technology designed for the high-speed transfer of voice, video, and data through public and private networks using cell relay technology. ATM is an International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard. Ongoing work on ATM standards is being done primarily by the ATM Forum, which was jointly founded by Cisco Systems, NET/ADAPTIVE, Northern Telecom, and Sprint in 1991.

A cell switching and multiplexing technology, ATM combines the benefits of circuit switching (constant transmission delay, guaranteed capacity) with those of packet switching (flexibility, efficiency for intermittent traffic). To achieve these benefits, ATM uses the following features:

- Fixed-size cells, permitting more efficient switching in hardware than is possible with variable-length packets
- Connection-oriented service, permitting routing of cells through the ATM network over virtual connections, sometimes called virtual circuits, using simple connection identifiers
- Asynchronous multiplexing, permitting efficient use of bandwidth and interleaving of data of varying priority and size

The combination of these features allows ATM to provide different categories of service for different data requirements and to establish a service contract at the time a connection is set up. This means that a virtual connection of a given service category can be guaranteed a certain bandwidth, as well as other traffic parameters, for the life of the connection.

For more details on ATM Technology, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/12_1/pereg_1/atm_tech/index.htm

DSL Technology

Digital Subscriber Line (DSL) is a public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: Asymmetric DSL (ADSL), High-Data-Rate DSL (HDSL), Single-line DSL (SDSL), and Very-high-data-rate DSL (VDSL). All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

For more details on DSL Technology, refer to the following URL:

http://www.cisco.com/en/US/tech/tk175/tsd_technology_support_category_home.html

How to Enable Monitoring and Retraining on Reception of Loss of Margin Messages

Enabling LOM Monitoring

To enable LOM monitoring, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number*
4. **dsl lom** number *number*
5. **end**
6. **show dsl interface atm**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface atm** *interface-number* **Example:** `Router(config)# interface atm 3`	Configures an ATM interface and enters interface configuration mode.
Step 4	**dsl lom** number *number* **Example:** `Router(config-if)# dsl lom 200`	Enables LoM monitoring and checks for the specified number of consecutive LoM messages.
Step 5	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show dsl interface atm** **Example:** `Router# show dsl interface atm`	Verifies the LOM monitoring configuration.

Configuration Examples for Monitoring and Retraining on Reception of Loss of Margin Messages

- Enabling LoM Monitoring Example, page 466

Enabling LoM Monitoring Example

The following example shows LoM monitoring enabled on an ATM interface with retraining configured for 200 counts:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
interface atm0
dsl lom 200
end
!
show run interface atm0
00:16:46: %SYS-5-CONFIG_I: Configured from console by consoleint a0
Building Configuration
Current configuration: 209 bytes
!
interface atm0
ip address 1.2.3.4 255.255.255.0
no atm ilmi-keepalive
pvc 1/40
protocol ip 1.2.3.5 broadcast
encapsulation aal5snap
!
dsl operating-mode auto
dsl lom 200
dsl power-cutback 0
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Release 12.3 Configuration Guides and Command References	Cisco IOS Release 12.3 Configuration Guides and Command References

Standards

Standards	Title
None	--

MIBs

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

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Feature Information for Monitoring and Retraining on Reception of Loss of Margin Messages

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

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

Table 37 Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Monitoring and Retraining on Reception of Loss of Margin Messages	12.3(2)T	Loss of Margin (LoM) monitoring allows the router to handle asymmetric digital subscriber line (ADSL) loss of margin messages received from the digital subscriber line access multiplexer (DSLAM). The **dsl lom** command is used to set digital subscriber line (DSL) LoM monitoring. The **no dsl lom** command disables LoM monitoring after the router has been configured to monitor LoM messages. When set to monitor LoM, the router will retrain with the DSLAM when it receives LoM messages consecutively for the number of times specified in the *number* argument. The following command was introduced or modified: **dsl lom**.

Virtual Auxiliary Port Feature and Configuration of DSL Settings

The virtual auxiliary port feature provides support for dial backup and out-of-band management on Cisco 837 and Cisco 831 routers, and provides support for out-of-band management on Cisco SOHO 97 and Cisco SOHO 91 routers. On these routers, the console port and the auxiliary port share the same physical RJ-45 port. The console port must be changed to act as a virtual auxiliary port, using the command-line interface (CLI) before the dial backup and out-of-band management capabilities can be enabled.

In addition, digital subscriber line (DSL) settings can now be configured on the Cisco 837, Cisco 831, Cisco SOHO 97, and Cisco SOHO 91 routers by using the DSL settings commands.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About the Virtual Auxiliary Port

When the virtual auxiliary port is enabled, the signals directed from the RJ-45 pins are processed by the auxiliary port driver, and the console port is disabled. The virtual auxiliary port can be used to provide the standard Cisco IOS interactive user interface.

How to Configure the Virtual Auxiliary Port and the DSL Settings

Configuring the Virtual Auxiliary Port

Perform these steps to configure the virtual auxiliary port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line con0**
4. **modem 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	**line con0** **Example:** `Router(config)# line con0`	Enters line configuration mode for the console interface.
Step 4	**modem enable** **Example:** `Router(config-line)# modem enable`	Changes the console port to function as an auxiliary port.

Configuring the DSL Settings

Perform these steps to configure the DSL settings.

Note For each DSL setting to take effect, the asymmetric digital subscriber line (ADSL) driver resets the ADSL subsystem, which causes the firmware to be downloaded again.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm0**
4. **dsl noise-margin** *decimal*
5. **end**
6. **enable**
7. **configure terminal**
8. **interface atm0**
9. **dsl max-tone-bits** *integer*
10. **end**
11. **enable**
12. **configure terminal**
13. **interface atm0**
14. **dsl gain-setting tx-offset** *decimal*
15. **end**
16. **enable**
17. **configure terminal**
18. **interface atm0**
19. **dsl gain-setting rx-offset** *decimal*
20. **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 atm0** **Example:** `Router(config)# interface atm0`	Enters interface configuration mode.
Step 4	**dsl noise-margin** *decimal* **Example:** `Router(config-if)# dsl noise-margin 0.5`	Sets the noise margin offset. • *Decimal* ranges from -3 dB to 3 dB with a granularity of 0.5 dB.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and resets the ADSL subsystem.
Step 6	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 7	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 8	**interface atm0** **Example:** `Router(config)# interface atm0`	Enters interface configuration mode.

	Command or Action	Purpose
Step 9	**dsl max-tone-bits** *integer* **Example:** `Router(config-if)# max-tone-bits 10`	Sets the maximum bits per tone limit. • *Integer* ranges from 2 dB to 14 dB with a granularity of 1 dB.
Step 10	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and resets the ADSL subsystem.
Step 11	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 12	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 13	**interface atm0** **Example:** `Router(config)# interface atm0`	Enters interface configuration mode.
Step 14	**dsl gain-setting tx-offset** *decimal* **Example:** `Router(config-if)# dsl gain-setting tx-offset 0`	Sets the transmit gain offset. • *Decimal* ranges from -10 dB to 3 dB with a granularity of 0.5 dB.
Step 15	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and resets the ADSL subsystem.

	Command or Action	Purpose
Step 16	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 17	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 18	**interface atm0** **Example:** `Router(config)# interface atm0`	Enters interface configuration mode.
Step 19	**dsl gain-setting rx-offset** *decimal* **Example:** `Router(config-if)# dsl gain-setting rx-offset 1`	Sets the receive gain offset. • *Decimal* ranges from -5 dB to 3 dB with a granularity of 0.5 dB.
Step 20	**end** **Example:** `Router(config-if)# end`	Ends the configuration mode.

Configuration Example for Configuring the DSL Settings

```
interface atm0
no ip address
dsl noise-margin 0
dsl max-tone-bits 14
dsl gain-setting tx-offset 0
dsl gain-setting rx-offset 1
```

Additional References

Related Documents

Related Topic	Document Title
Configuring Dial Backup	*Cisco 826, 827, 828, 831, 836, and 837 and Cisco SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide*

Standards

Standards[9]	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	

MIBs

MIBs[10]	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 IOS releases, and feature sets, use Cisco MIB Locator available at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs[11]	Title
No new or modified RFCs are supported by this feature. Support for existing RFCs has not been modified by this feature.	

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

9 Not all supported standards are listed.
10 Not all supported MIBs are listed.
11 Not all supported RFCs are listed.

Feature Information for Configuring the DSL Settings

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

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

Table 38 Feature Information for Phrase Based on Module Title

Feature Name	Releases	Feature Information
Virtual Auxiliary Port Feature and Configuration of DSL Settings	12.2(8)YN 12.3(2)T	The virtual auxiliary port feature provides support for dial backup and out-of-band management on Cisco 837 and Cisco 831 routers, and provides support for out-of-band management on Cisco SOHO 97 and Cisco SOHO 91 routers. On these routers, the console port and the auxiliary port share the same physical RJ-45 port. The console port must be changed to act as a virtual auxiliary port, using the command-line interface (CLI) before the dial backup and out-of-band management capabilities can be enabled. In addition, digital subscriber line (DSL) settings can now be configured on the Cisco 837, Cisco 831, Cisco SOHO 97, and Cisco SOHO 91 routers by using the DSL settings commands. The following commands were introduced or modified: **modem enable**, **dsl max-tone-bits**, **dsl gain-setting rx-offset**, **dsl gain-setting rx-offset**, **dsl gain-setting tx-offset**, **dsl noise-margin**.