Broadband Access Aggregation and DSL Configuration Guide, Cisco IOS Release 12.2SR

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

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

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

Prerequisites for Providing 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.

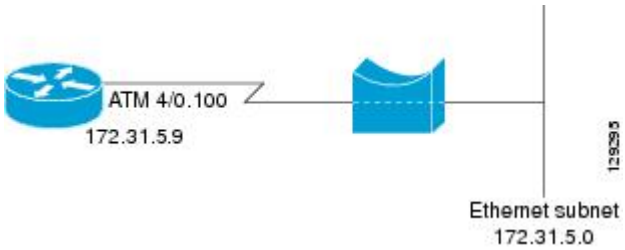
Information About Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs

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 1 ATM Routed Bridge Encapsulation



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

ATM RBE Subinterface Grouping by PVC Range

You can configure ATM routed bridge encapsulation using an ATM PVC range rather than individual PVCs. When you configure a PVC range for routed bridge encapsulation, a point-to-point subinterface is created for each PVC in the range. The number of PVCs in a range can be calculated using the following formula:

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.

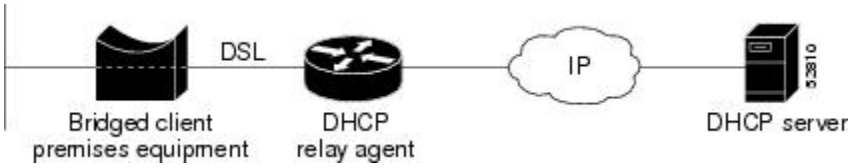
Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

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.

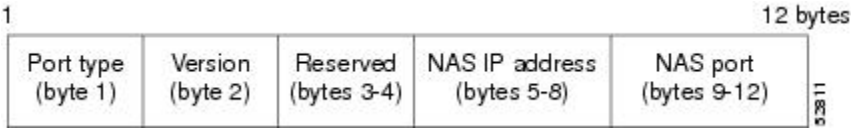
Figure 2 Network Topology Using ATM RBE and DHCP



This feature communicates information to the DHCP server using a suboption of the DHCP relay agent information option called agent remote ID. The information sent in the agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

The figure below shows the format of the agent remote ID suboption.

Figure 3 Format of the Agent Remote ID Suboption



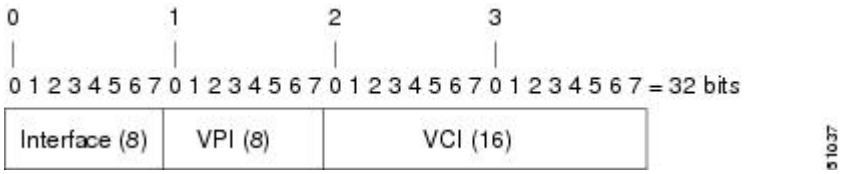
The table below describes the agent remote ID suboption fields displayed in the figure above.

Table 1 Agent Remote ID Suboption Field Descriptions

Field	Description
Port Type	Port type. The value 0x01 indicates RBE. (1 byte)
Version	Option 82 version. The value 0x01 specifies the RBE version of Option 82 (1 byte).
Reserved	RBE reserved (2 bytes).
NAS IP Address	One of the interfaces on the DHCP relay agent. The **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)

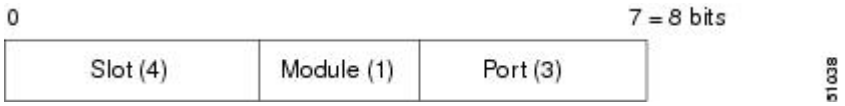
The figure below shows the format of the network access server (NAS) port field in the agent remote ID suboption.

Figure 4 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 5 Format of the Interface Field



DHCP Lease Limit per ATM RBE Unnumbered Interface

The DHCP lease limit per ATM RBE Unnumbered Interface feature is enabled on a Cisco IOS DHCP relay agent connected to clients through unnumbered interfaces. The relay agent keeps information about the DHCP leases offered to the clients per subinterface. When a DHCPACK message is forwarded to the client, the relay agent increments the number of leases offered to clients on that subinterface. If a new DHCP client tries to obtain an IP address and the number of leases has already reached the configured lease limit, DHCP messages from the client will be dropped and will not be forwarded to the DHCP server.

If this feature is enabled on the Cisco IOS DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new

client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

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

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 2 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 3 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**

NAS-Port-ID Format C Enhancement

The NAS-Port-ID Format C Enhancement feature introduces the **nas-port-id format c** command for Broadband Access Group (BBA group) configuration. This command defines a specific broadband subscriber access line identification (NAS-Port-ID) coding format. When this command is configured, the original value of the NAS-Port-ID tag is overwritten. If no valid string is available for the Remote-ID or the Circuit-ID tag as part of Dynamic Host Configuration Protocol (DHCP) option 82, a default string of 0/0/0/0/0/0 is appended to the NAS-Port-ID tag.

Finding Feature Information

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

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

Prerequisites for NAS-Port-ID Format C Enhancement

The NAS-Port-ID tag is created.

Restrictions for NAS-Port-ID Format C Enhancement

The NAS-Port-ID Format C Enhancement feature is supported on the Cisco 10000 series platform where PPP over Ethernet (PPPoE) server functionality is supported.

This feature is not supported on PPP over ATM.

Information About NAS-Port-ID Format C Enhancement

Coding Format for NAS-Port-ID Format C

The NAS-Port-ID Format C Enhancement feature provides the following broadband subscriber access line identification (NAS-Port-ID) coding format:

{atm/eth/trunk} NAS_slot/NAS_subslot/NAS_port:XPI:XCI {Circuit-ID/Remote-ID/default string}

- For ATM, XPI is the virtual path identifier (VPI) and XCI is the virtual circuit identifier (VCI).
- For Ethernet, XPI is outer vlan-tag, XCI is inner vlan-tag.
- Requirements for XPI:XCI for Ethernet are as follows:
  - For 802.1Q tunneling (QinQ), the format should be outer vlan-tag:inner vlan-tag. (Prior to Release 12.2(31)SB2, Cisco IOS software supports inner vlan-tag:outer vlan-tag).
  - For single tag VLAN, XPI should be 4096.
- The Circuit-ID tag (if present) must be appended to this string when the **nas-port-id format c** command is used. The format for the Circuit-ID or Remote-ID tag is as follows:

AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]

- The digital subscriber line access multiplexer (DSLAM) should append this information to the broadband remote access server (BRAS), and the BRAS transparently delivers it. If the Circuit-ID or Remote-ID tag is not present in DHCP option 82, a string of 0/0/0/0/0/0 should be appended to the NAS-Port-ID tag.

The following examples illustrate this format:

- NAS-Port-ID = atm 31/31/7:255.65535 name001/0/31/63/31/127

In this example, the subscriber interface type of the BRAS equipment is an ATM interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the VPI is 255, and the VCI is 65535. The string name001/0/31/63/31/127 is the Circuit-ID or Remote-ID tag.

- NAS-Port-ID = eth 31/31/7:1234.2345 0/0/0/0/0/0

In this example, the subscriber interface type of the BRAS equipment is an Ethernet interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the outer vlan-tag is 1234, and the inner vlan-tag is 2345. The string 0/0/0/0/0/0 is the default.

- NAS-Port-ID = eth 31/31/7:4096.2345 0/0/0/0/0/0

In this example, the subscriber interface type of the BRAS equipment is an Ethernet interface, the BRAS slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, and the VLAN ID is 2345. The string 0/0/0/0/0/0 is the default.

How to Configure the NAS-Port-ID Format C Enhancement Feature

Configuring the NAS-Port-ID Format C Enhancement Feature

To overwrite the original value of the NAS-Port-ID tag and define the specific broadband subscriber access line identification (NAS-Port-ID) coding format perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **virtual-template** *template-number*
5. **nas-port-id format c**
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* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.

	Command or Action	Purpose
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual access interfaces.
Step 5	**nas-port-id format c** **Example:** `Router(config-bba-group)# nas-port-id format c`	Specifies a format for broadband subscriber access line identification coding. **Note** The designation of **format c** is specifically designed as follows: NAS_PORT_ID=atm 31/31/7:255.65535 name001/0/31/63/31/127
Step 6	**end** **Example:** `Router(config-bba-group)# end` **Example:**	Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for NAS-Port-ID Format C Enhancement

To enable the NAS-Port-ID Format C Enhancement feature, you must configure the access concentrator side and the client side in your network. :

- Configuring PPPoE over Ethernet for the Access Concentrator Side and Client Side Example, page 20
- Configuring PPPoE over ATM AAL5 SNAP for the Access Concentrator Side and Client Side Example, page 21

Configuring PPPoE over Ethernet for the Access Concentrator Side and Client Side Example

The following is a sample configuration for the access concentrator side of a PPPoE over Ethernet configuration:

```
bba-group pppoe bba-pppoeoe
 virtual-template 1
 nas-port-id format c
!
interface Loopback0
```

```
 ip address 209.165.200.234 255.255.255.224
!
interface Virtual-Template1
 ip unnumbered Loopback0
no peer default ip address
 ppp authentication chap
!
interface FastEthernet0/0
 description PPPoEoE
 pppoe enable group bba-pppoeoe
!
```

The following is a sample configuration for the client side:

```
bba-group pppoe bbag-pppoeoe
 virtual-template 1
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ppp chap hostname xyz
 ppp chap password 0 lab
!
interface Loopback0
 ip address 209.165.200.243 255.255.255.224
!
interface FastEthernet1/1
 no ip address
 pppoe enable group bbag-pppoeoe
!
```

Configuring PPPoE over ATM AAL5 SNAP for the Access Concentrator Side and Client Side Example

The following is a sample configuration for the access concentrator side of a PPPoE over an ATM/AAL5 Subnetwork Access Protocol (SNAP) configuration:

```
bba-group pppoe bba-pppoeoa
 virtual-template 2
 nas-port-id format c
!
interface Loopback1
 ip address 209.165.200.245 255.255.255.224
!
interface Virtual-Template2
 ip unnumbered Loopback1
no peer default ip address
 ppp authentication chap
!
interface ATM2/0.1 multipoint
 description PPPoEoA
 pvc 1/100
  encapsulation aal5snap
  protocol pppoe group bba-pppoeoa
 !
```

The following is a sample configuration for the client side:

```
bba-group pppoe bbag-pppoeoa
 virtual-template 2
!
interface Virtual-Template2
 ip unnumbered Loopback1
 ppp chap hostname abc
 ppp chap password 0 lab
!
interface Loopback1
 ip address 209.165.200.247 255.255.255.224
!
```

```
interface ATM6/0.1 multipoint
 pvc 1/100
 encapsulation aal5snap
 protocol pppoe group bbag-pppoeoa
 !
```

Additional References

The following sections provide references related to the NAS-Port-ID Format C Enhancement feature.

Related Documents

Related Topic	Document Title
Command reference documentation for commands used in this document	*Cisco IOS Broadband Access Aggregation and DSL Command Reference*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for NAS-Port-ID Format C Enhancement

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

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

Table 4 Feature Information for the NAS-Port-ID Format C Enhancement Feature

Feature Name	Releases	Feature Information
NAS-Port-ID Format C Enhancement	12.2(31)SB2 15.0(1)M	This feature supports Cisco 10000 series platform. The **nas-port-id format c**command defines a specific broadband subscriber access line identification (NAS-Port-ID) coding format. When this command is configured, the original value of the NAS-Port-ID tag is overwritten. If no valid string is available for the Remote-ID or Circuit-ID tag as part of Dynamic Host Configuration Protocol (DHCP) option 82, a default string of 0/0/0/0/0/0 is appended to the NAS-Port-ID tag. The following commands were introduced or modified: **nas-port-id format c**

Glossary

AAA --authentication, authorization, and accounting.

ATM --Asynchronous Transfer Mode.

BRAS --broadband remote access server.

CLI --command-line interface.

DHCP --Dynamic Host Configuration Protocol.

DSLAM --digital subscriber line access multiplexer.

HA --high availability.

NAS --network access server.

PPP --Point-to-Point Protocol

PPPoA --Point-to-Point Protocol over ATM.

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

QinQ --IEEE 802.1Q tunneling.

RADIUS --Remote Authentication Dial-In User Service (RFC 2865).

SNAP --Subnetwork Access Protocol.

VCI --virtual circuit identifier.

VLAN --virtual local-area network.

VPI --virtual path identifier.

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

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

Prerequisites for 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

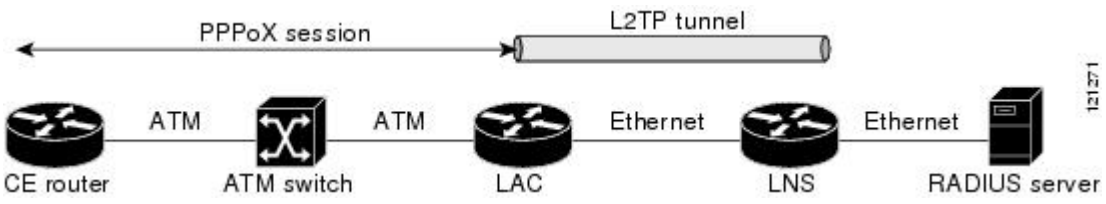
The send speed from the LAC to the remote destination is copied into AV pair 38 so that the session is symmetric at the LNS. The LNS does not do any policing of the upstream rate but verifies the session speed against the Service Level Agreement (SLA) before accepting it.

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 6 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

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

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 5 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.

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

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

Restrictions for 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

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 6 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.

PPP-Max-Payload and IWF PPPoE Tag Support

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

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

Finding Feature Information

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

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

Prerequisites for the PPP-Max-Payload and IWF PPPoE Tag Support Feature

To enable the PPP-Max-Payload and IWF PPPoE Tag Support feature, you should have configured PPPoE profile.

Restrictions for the PPP-Max-Payload and IWF PPPoE Tag Support Feature

PPPoE peers can negotiate only MRUs with a maximum of 1492 octets so that the PPPoE header and PPP protocol ID can be inserted in the PPPoE session data packet.

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

Accommodating an MTU MRU Greater than 1492 in PPPoE

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

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

Interworking Functionality

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

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

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

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

Enabling the PPP-Max-Payload and IWF PPPoE Tag Support Feature

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.
Step 4	**virtual-template** *template-number* **Example:** `Router(config-bba-group)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.
Step 5	**tag ppp-max-payload** [**minimum** *value* **maximum** *value*] [**deny**] **Example:** `Router(config-bba-group)# tag ppp-max-payload minimum 1200 maximum 3000`	Specifies a range for the ppp-max payload tag value that will be accepted by the BRAS. • Default values are 1492 for the minimum and 1500 for the maximum. • The ppp-max-payload tag value accepted from the client cannot exceed the physical interface value for MTU minus 8.
Step 6	**sessions per-mac limit** *per-mac-limit* **Example:** `Router(config-bba-group)# sessions per-mac iwf limit 200`	Specifies a limit for IWF-specific sessions per MAC address (separate from session limits that are not IWF-specific). • If this command is not entered, the normal MAC-address session limit is applied to IWF sessions. • The *per-mac-limit* argument specifies the allowable number of IWF sessions. The default is 100.
Step 7	**interface ethernet** *slot* / *port* **Example:** `Router(config-bba-group)# interface ethernet 1/0`	Enters interface configuration mode for an Ethernet interface: • The *slot* / *port* arguments identify the slot number and the port number to which this configuration applies. • The slash mark is required.
Step 8	**pppoe enable group** *group-name* **Example:** `Router(config-if)# pppoe enable group 1`	Enables PPPoE sessions on an Ethernet interface or subinterface.

	Command or Action	Purpose
Step 9	**virtual-template** *template-number* **Example:** `Router(config-if)# virtual-template 1`	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces. • The *template-number* argument is an identifying number of the virtual template that will be used to clone virtual-access interfaces.
Step 10	**ppp lcp echo mru verify** [**minimum** *value*] **Example:** `Router(config-if)# ppp lcp echo mru verify minimum 1304`	Verifies the negotiated MRU and adjusts the PPP virtual access interface MTU for troubleshooting purposes. • If the optional **minimum** keyword is entered, the *value* can be from 64 to 1500. • If the verification of minimum MTU succeeds, the PPP connection's interface MTU is set to that value. This reset is useful when you troubleshoot and need to adjust the sessions according to underlying physical network capability. After this command is configured, IP Control Protocol (IPCP) is delayed until verification of the MTU is completed at the LCP.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.
Step 12	**show pppoe session** [**all**| **packets**] **Example:** `Router# show pppoe session all`	Verifies the configuration and displays session information. • **all** --Displays output indicating if a session is IWF-specific or if the PPP-Max-Payload tag is in the discovery frame and accepted. • **packets** --Displays packet statistics for the PPPoE session.

Disabling the PPP-Max-Payload and IWF PPPoE Tag Support Feature

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **tag ppp-max-payload deny**
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 interface configuration mode.
Step 3	**bba-group pppoe** *group-name* **Example:** `Router(config-if)# bba-group pppoe pppoe-group`	Enters BBA group configuration mode and defines a PPPoE profile.
Step 4	**tag ppp-max-payload deny** **Example:** `Router(config-bba-group)# tag ppp-max-payload deny`	Disables the processing of the ppp-max-payload tag value higher than the default of 1492 bytes.
Step 5	**end** **Example:** `Router(config-bba-group)# end`	Exits the BBA group configuration mode and returns to privileged EXEC mode.

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

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

• Configuration with the PPP-Max-Payload and IWF PPPoE Tag Support Feature Enabled Example, page 57
• Configuration with the PPP-Max-Payload and IWF PPPoE Tag Support Feature Disabled Example, page 57

Configuration with the PPP-Max-Payload and IWF PPPoE Tag Support Feature Enabled Example

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

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

Configuration with the PPP-Max-Payload and IWF PPPoE Tag Support Feature Disabled Example

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

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

Additional References

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

Related Documents

Related Topic	Document Title
Command reference information for broadband and DSL	Cisco IOS Broadband Access Aggregation and DSL Command Reference

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS 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)
Draft RFC document	Accommodating an MTU/MRU Greater than 1492 in PPPoE

Technical Assistance

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

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

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

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

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

Feature Name	Releases	Feature Information
PPP-Max Payload and IWF PPPoE Tag Support	12.2(31)SB2 12.2(33)SRC 15.0(1)M	The PPP-Max-Payload and IWF PPPoE Tag Support feature enables the PPP over Ethernet (PPPoE) component to process the PPP-Max-Payload and Interworking Functionality (IWF) PPPoE tags in the PPPoE discovery frame: • The **tag ppp-max-payload** command allows PPPoE peers to negotiate PPP maximum receive units (MRUs) greater than 1492 octets if the underlying network supports a maximum transmission unit (MTU) size greater than 1500 octets. • The IWF PPPoE tag allows the Broadband Remote Access Server (BRAS) to distinguish the IWF PPPoE from the regular PPPoE sessions to overcome the per-MAC session limit put on the BRAS as a protection from denial of service (DOS) attacks sourced from the same MAC address. The following commands were introduced or modified: **ppp lcp echo mru verify** , **tag ppp-max-payload**

Glossary

BBA --Broadband access.

BRAS --Broadband Remote Access Server, typically acting as a PPPoE server.

DOS --Denial of service (a form of security attacks).

DSLAM --Digital subscriber line access multiplexer.

IPCP --IP Control Protocol.

IWF --Interworking Functionality (used to describe the PPPoA conversion to PPPoE sessions at the DSLAM).

IWF PPPoE session --A PPPoE session from the DSLAM to the BRAS that is actually a PPPoA session from the end user to the DSLAM.

LCP --Link Control Protocol.

MRU --PPP maximum received unit as negotiated in LCP.

MTU --Maximum transmission unit of an interface.

PADO --PPPoE Active Discovery Offer.

PADR --PPPoE Active Discovery Request.

PADS --PPPoE Active Discovery Session Confirmation.

PPP --Point-to-Point Protocol

PPPoE --PPP over Ethernet protocol or PPPoE component.

VPDN --virtual private dialup network.

PPPoE - Session Limit Local Override

The PPP over Ethernet (PPPoE) Session Limit Local Override feature enables the session limit configured locally on the broadband remote access server (BRAS) or Layer2 Tunneling Protocol (L2TP) access concentrator (LAC) to override the per-NAS-port session limit downloaded from the RADIUS server when the preauthorization is enabled.

Finding Feature Information

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

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

Information About PPPoE Session Limit Local Override

How PPPoE Session Limit Local Override Works

PPPoE session limits are downloaded from the RADIUS server when you enable preauthorization on the LAC using the **subscriber access pppoe pre-authorize nas-port-id** command. By enabling preauthorization, you limit the number of PPPoE sessions on a specific permanent virtual circuit (PVC) or VLAN; that is, the PPPoE per-NAS-port session limit downloaded from the RADIUS server takes precedence over locally configured (port-based) session limits, such as per-VC and per-VLAN session limits.

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

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

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

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

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

For more information on how to configure preauthorization and per-NAS-port session limit, see the Establishing PPPoE Session Limit per NAS Port document.

How to Configure PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override

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

The **sessions pre-auth limit ignore** command should have been configured under the broadband access (BBA) group associated with the interface.

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

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bba-group pppoe** *group-name*
4. **sessions per-vc limit** *per-vc-limit*
5. **sessions pre-auth limit ignore**
6. **end**

DETAILED STEPS

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

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

Configuration Examples for PPPoE Session Limit Local Override

Enabling PPPoE Session Limit Local Override Example

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

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

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

Additional References

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

Related Documents

Related Topic	Document Title
Establishing PPPoE Session Limits per NAS Port	Cisco IOS Broadband Access Aggregation and DSL Configuration Guide

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

Technical Assistance

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

Feature Information for PPPoE Session Limit Local Override

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

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

Table 8 Feature Information for PPPoE Session Limit Local Override

Feature Name	Releases	Feature Information
PPPoE Session Limit Local Override	12.4(15)T 12.2(33)SB 15.0(1)M 12.2(33)SRE	The PPPoE Session Limit Local Override feature enables the local session limit configured on the BRAS or LAC to override the per-NAS-port session limit downloaded from the RADIUS server when preauthorization is configured. The following command was introduced by this feature: **sessions pre-auth limit ignore** In Cisco IOS Release 12.2(33)SB, support was added for the Cisco 10000 router.

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

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

Information About 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

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 9 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**