Cisco IOS Broadband Access Aggregation and DSL Command Reference

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

CONTENTS

ac name through logging rate-limit

access-list template

To enable template access control list (ACL) processing (as defined by the Template ACL feature), use the **access-list template** command in global configuration mode. To disable template ACL processing, use the **no** form of this command.

access-list template [*number-of-rules*]

no access-list template [*number-of-rules*]

Syntax Description

number-of-rules	(Optional) Specifies the maximum number of rules that an ACL may have in order to be considered for template status, that is, considered as a template ACL. Only ACLs whose number of rules is the same as or smaller than those specified in the *number-of-rules*argument will be considered for template status. If the *number-of-rules*argument is omitted, the default of 100 will be used, and only ACLs with 100 or fewer rules will be considered for template status. The range for the *number-of-rules*argument is from 1 to 100.

Command Default

Template ACL processing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(27)SBKA	This command was introduced on the Cisco 10000 series router.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Reducing the number of rules for template ACL status can lower CPU utilization. Checking each ACL against other known ACLs in the system is easier if the matching task can be aborted earlier.

Note Changes in CPU utilization occur only during session initialization. Steady-state CPU utilization is unaffected by these changes in ACL processing.

If template ACL processing is disabled, the system replaces all existing template ACL instances with ACLs. Therefore, before you disable the feature, you must ensure that the number of template ACLs does not exceed the system capabilities.

If template ACL processing is enabled, the system scans and evaluates all configured per-session ACLs, and then creates all required template ACLs.

Default Settings

If the number-of-rules argument is specified for the no version of the command, the default of 100 will be used, and only ACLs with 100 or fewer rules will be considered for template status.

Cisco 1000 Series Routers

On the Cisco 1000 series routers, if the number of rules is smaller than the largest similar Attribute 242 ACL, the processing of this new setting can use up substantial CPU resources because ACLs that previously would be considered as template ACL duplicates are instead compiled using TurboACL compilation without regard to other ACLs already in the router. If the ACLs have fewer than eight rules, the CPU increase will not be so noticeable, because ACLs will be compiled as MiniACLs.

If the number of rules is set larger than the largest similar Attribute 242 ACL, then increased CPU resources may be required to conduct the comparison task. This potential increase in CPU resources is offset by the elimination of TurboACL and MiniACL compilation.

Examples

The following example specifies that ACLs with 50 or fewer rules will be considered for template ACL status:

```
Router(config)# access-list template 50
```

ac name

To specify the name of the access concentrator to be used in PPPoE Active Discovery Offers (PADO), use the **ac name** command in BBA group configuration mode. To remove this specification, use the **no** form of this command.

ac name *name*

no ac name *name*

Syntax Description

name	Name of the access concentrator to be used in PADOs.

Command Default

If the name of the access concentrator is not specified, the name of the router is used as the access concentrator name.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **ac name** command allows you to advertise a unique access concentrator name other than the router name to PPPoE clients.

Examples

The following example shows the configuration of the name "region1" as the access concentrator name to be used in PADOs:

```
bba-group pppoe global
 virtual-template 1
 ac name region1
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

atm pppatm link reset

To configure the system to bring down PPP over ATM (PPPoA) sessions when the virtual circuit (VC) is deactivated, use the **atm pppatm link reset** command in subinterface configuration mode. To return to the default behavior (PPPoA sessions are not brought down), use the **no** form of this command.

atm pppatm link reset

no atm pppatm link reset

Syntax Description

This command has no arguments or keywords.

Command Default

PPPoA sessions are not brought down when the VC is deactivated.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

Use the **atm pppatm link reset** command to configure the system to place PPPoA sessions in a nonoperational state when a VC is deactivated. This command is useful on customer premises equipment (CPE) that is not configured with Dialer. On L2TP access concentrators (LACs), issues of scalability make it useful to allow PPPoA sessions to remain up when a VC is deactivated.

Examples

In the following example, PPPoA sessions on permanent virtual circuit (PVC) 3/501 will be brought down when that PVC is deactivated:

```
interface ATM4/0
 atm pppatm link reset
 pvc 3/501
  encapsulation aal5snap
  protocol ppp virtual-template 1
 !
interface virtual-template 1
 no ip address
 ppp chap hostname boston
 ppp chap password 7 111F1111
 ppp multilink
 ppp multilink group 1
interface multilink1
 ip unnumbered loopback 0
 ppp multilink
 ppp multilink group 1
```

atm route-bridged

To configure an interface to use the ATM routed bridge encapsulation (RBE), use the **atm route-bridged**command in interface configuration mode.

atm route-bridged *protocol*

Syntax Description

protocol	Protocol to be route-bridged. IP and IPv6 are the only protocols that can be route-bridged using ATM RBE.

Command Default

ATM routed bridge encapsulation is not configured.

Command Modes

ATM subinterface configuration

Command History

Release	Modification
12.0(5)DC	This command was introduced.
12.1(2)T	This command was integrated in Cisco IOS Release 12.1(2)T.
12.3(4)T	The **ipv6** keyword was added to support RBE of IPv6 packets as specified in RFC 1483.
12.4(2)T	This command was updated to work with QoS policy-based routing in Cisco IOS Release 12.4(2)T.
Cisco IOS XE Release 3.2S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use this command to configure RBE on an ATM interface. The **atm route-bridged**command can also be used to integrate RBE with quality of service (QoS) features on the Cisco 800 and 1700 series routers.

Routing of IPv6 and IP Packets

IP and IPv6 packets can be routed using RBE only over ATM point-to-point subinterfaces.

Routing of IP packets and IPv6 half-bridging, bridging, PPP over Ethernet (PPPoE), or other Ethernet 802.3-encapsulated protocols can be configured on the same subinterface.

Router Advertisements with IPv6

Router advertisements are suppressed by default. For stateless autoconfiguration, router advertisements must be allowed with the **no ipv6 nd suppress-ra** command. For static configuration, router advertisement is not required; however, the aggregator should either have the RBE interface on the same subnet as the client or have a static IPv6 route to that subnet through the RBE interface.

Examples

Examples

The following example configures ATM routed bridge encapsulation on an interface:

```
interface atm 4/0.100 point-to-point
 ip address 172.16.5.9 255.255.255.0
 atm route-bridged ip
 pvc 0/32
```

Examples

The following example shows a typical configuration on an RBE interface to allow routing of IPv6 encapsulated Ethernet packets. IPv6 packets sent out of the subinterface are encapsulated over Ethernet over the RBE interface.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 no ipv6 nd suppress-ra
 atm route-bridged ipv6
 pvc 1/101
```

In this example, the **ipv6 enable** command allows the routing of IPv6 packets. The **ipv6 address** command specifies an IPv6 address for the interface and an IPv6 prefix to be advertised to a peer. The **no ipv6 nd ra suppress** command enables router advertisements on the interface.

Examples

The following example shows a configuration in which IPv6 packets are routed and all other packets are bridged.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 atm route-bridged ipv6
 bridge-group 1
 pvc 1/101
```

Examples

IP and IPv6 routing can be configured on the same interface as shown in this example. All other packets are bridged. PPPoE could also be configured on this same interface.

```
interface ATM1/0.1 point-to-point
 ipv6 enable
 ipv6 address 3FEE:12E1:2AC1:EA32::/64
 ip address 10.0.0.1 255.255.255.0
 atm route-bridged ipv6
 atm route-bridged ip
 bridge-group 1
 pvc 1/101
```

Examples

The following example shows the IPv6 static route configured. Unlike IP, the IPv6 interface on an aggregator is always numbered and, minimally, has a link local IPv6 address.

```
Router# configure terminal
Router(config)# ipv6 route 3FEE:12E1:2AC1:EA32::/64 atm1/0.3
Router(config)# end
```

Examples

Notice in this **show ipv6 interface** output display that each RBE link has its own subnet prefix. Unlike proxy ARP in IPv4 RBE configurations, the aggregator does not require proxy ND in IPv6 RBE deployments.

```
Router# show ipv6 interface atm1/0.1
ATM1/0.1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE3B:B400
  Global unicast address(es):
    3FEE:12E1:2AC1:EA32::, subnet is 3FEE:12E1:2AC1:EA32::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FF3B:B400
  MTU is 4470 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses
```

Examples

The following partial example configures a single PVC using AAL5SNAP encapsulation and class-based routing for traffic shaping on the interface where RBE is enabled. The following CBWFQ parameters are configured: access-list with different IP precedence, class map, policy map, and service policy. Different bandwidth classes are configured in the same policy.

RBE base configuration:

```
interface FastEthernet0
 ip address 172.22.1.1 255.255.0.0
!
interface ATM0.1 point-to-point
 ip address 10.1.1.5 255.255.255.252
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
interface ATM0.1 point-to-point
 ip address 10.1.1.1 255.255.255.252
 atm route-bridged ip
 pvc 99/900
  encapsulation aal5snap
!
interface ATM0.1 point-to-point
 ip address 172.18.0.1 255.0.0.0
 pvc 100/1000
!
router eigrp 100
 network 10.1.0.0
 network 172.18.0.0
 network 172.22.0.0
.
.
.
```

CBWFQ configuration:

```
class-map match-all voice
 match access-group 105
!
policy-map voicedatapolicy
 class voice
```

```
  bandwidth 200
 class class-default
  fair-queue
  random-detect
!
interface Ethernet0
 ip address 172.25.1.1 255.0.0.0
 hold-queue 600 in
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 ip address 10.2.3.4 255.255.255.0
 atm route-bridged ip
 pvc 1/42
  protocol ip 10.2.3.5 broadcast
  vbr-nrt 300 300
  encapsulation aal5snap
  service-policy output voicedatapolicy
.
.
.
```

Related Commands

Command	Description
no ipv6 nd ra suppress	Suppresses IPv6 router advertisement transmissions on a LAN interface.

bba-group pppoe

To create a PPP over Ethernet (PPPoE) profile, use the **bba-group pppoe** command in global configuration mode. To delete a PPPoE profile, use the **no** form of this command.

bba-group pppoe {*group-name*| **global**}

no bba-group pppoe {*group-name*| **global**}

Syntax Description

group-name	Name of the PPPoE profile.
global	PPPoE profile that serves as the default profile for any PPPoE port--Ethernet interface, VLAN, or permanent virtual circuit (PVC)--that has not been assigned a specific PPPoE profile.

Command Default

A PPPoE profile is not configured.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated.
12.2(28)SB	This command was integrated.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

PPPoE profiles contain the configuration for a group of PPPoE sessions. Once a profile has been defined, it can be assigned to a PPPoE port (Ethernet interface, VLAN, or PVC), a virtual circuit (VC) class, or an ATM PVC range. PPPoE profiles can also be used with PPP over ATM (PPPoA)/PPPoE autosense. Multiple PPPoE profiles can be created and assigned to different ports.

The global PPPoE profile serves as the default profile for any port that has not been assigned a specific PPPoE profile.

Examples

The following example shows the configuration of a global PPPoE profile and a profile called "vpn1". PPPoE sessions established on PVCs that use the VC class "class-pppoe-global" will use the global profile. PVCs in the range "range-pppoe-1" will use the "vpn1" profile.

```
Router(config)# bba-group pppoe global
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions max limit 8000
Router(config-bba-group)# sessions per-vc limit 8
Router(config-bba-group)# sessions per-mac limit 2
!
Router(config-bba-group)# bba-group pppoe vpn1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vc limit 2
Router(config-bba-group)# sessions per-mac limit 1
!
Router(config-bba-group)# vc-class atm class-pppoe-global
Router(config-bba-group)# protocol pppoe
!
Router(config-bba-group)# interface ATM1/0.10 multipoint
Router(config-bba-group)# range range-pppoe-1 pvc 100 109
Router(config-bba-group)# protocol pppoe group vpn1
!
Router(config-bba-group)# interface ATM1/0.20 multipoint
Router(config-bba-group)# class-int class-pppoe-global
Router(config-bba-group)# pvc 0/200
```

Related Commands

Command	Description
encapsulation aal5autoppp virtual-template	Enables PPPoA/PPPoE autosense.
pppoe enable	Enables PPPoE sessions on an Ethernet interface or subinterface.
protocol pppoe (ATM VC)	Enables PPPoE sessions to be established on PVCs.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.

call admission limit

To instruct Internet Key Exchange (IKE) to drop security association (SA) requests (that is, calls for Call Admission Control [CAC]) when a specified level of system resources is being consumed, use the **call admission limit** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission limit *charge*

no call admission limit *charge*

Syntax Description

charge	Level of the system resources that, when used, causes IKE to stop accepting new SA requests. Valid values are 1 to 100000.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To prevent IKE processes from using excessive CPU resources, you can set a limit value depending on the network topology, the capabilities of the router, and the traffic patterns.

Examples

The following example causes IKE to drop calls when a given level of system resources are being used:

```
Router(config)# call admission limit 90000
```

Related Commands

Command	Description
call admission load	Configures a CAC metric for scaling WAN protocol session load.

Command	Description
crypto call admission limit	Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests.
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

call admission load

To configure a call admission control (CAC) metric for scaling WAN protocol session load, use the **call admission load** command in global configuration mode. To disable this feature, use the **no** form of this command.

call admission load *multiplier metric-poll-rate*

no call admission load *multiplier metric-poll-rate*

Syntax Description

multiplier	Multiplier value that provides a scaling factor for determining total load. Valid values are from 1 to 1000, and the default is 100.
metric-poll-rate	Load metric poll rate, in seconds. Valid values are from 1 to 32 seconds, and the default is 1.

Command Default

The default values are 100 for the multiplier and 1 for the poll rate. These values should not be changed without guidance from Cisco technical personnel.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

This command enables CAC to limit overconsumption of Cisco IOS CPU cycles. On hardware-forwarded router platforms, established sessions tend not to consume much of the router processor resources, but there is a need to reduce resource utilization during session establishment, especially, to determine when a call cannot be handled and then to determine when it can be handled again.

For the **call admission load** command, the router load is calculated when software routines average the current CPU utilization. The command is configured as a mathematical formula--**call admission load** *multiplier metric-poll-rate*--where CPU utilization is polled every *metric-poll-rate*seconds and multiplied by a *multiplier*, which is the scaling factor. This formula results in a metric value for the current router load determined by existing sessions. The value is compared to that set for the **call admission limit** command, and if it exceeds the value, the call is rejected; otherwise, the call is accepted.

Note We suggest that you not modify the default values without guidance from Cisco technical personnel.

Examples

The following example shows recommended settings for the **call admission load** and **call admission limit** commands on the Cisco 10000 ESR:

```
Router(config)# call admission limit 90
Router(config)# call admission load 100 1
```

Related Commands

Command	Description
call admission limit	Invokes CAC to scale WAN protocol session limits based on the percentage of system resources being consumed.
clear call admission statistics	Clears call admission statistics.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

class-range

To assign a virtual circuit (VC) class to an ATM permanent virtual circuit (PVC) range, use the **class-range** command in PVC range configuration mode. To remove the VC class, use the **no** form of this command.

class-range *class-name*

no class-range *class-name*

Syntax Description

class-name	Name of the VC class.

Command Default

No VC class is assigned to the PVC range.

Command Modes

PVC range configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When you create a VC class for an ATM PVC range, you can use the following commands to define your parameters: **abr**, **broadcast**, **cbr**, **encapsulation aal5**, **ilmi manage**, **inarp**, **oam-pvc**, **oam retry**, **protocol**, **ubr**, **ubr+**, **vbr-nrt**, and **vbr-rt**.

Parameters that are configured for a PVC range through discrete commands entered in PVC range configuration mode supersede VC class parameters assigned to an ATM PVC range using the **class-range** command.

Examples

In the following example, a class called "classA" is created and then applied to an ATM PVC range called "range-pppoa-1":

```
! The following commands create the class classA:
vc-class atm classA
 ubr 10000
 encapsulation aal5snap

! The following commands apply classA to an ATM PVC range:
interface atm 6/0.110 multipoint
 range range-pppoa-1 pvc 0/102 0/199
  class-range classA
```

Related Commands

Command	Description
shutdown (PVC-in-range)	Deactivates an individual PVC within a PVC range.
shutdown (PVC range)	Deactivates an ATM PVC range.

clear call admission statistics

To clear call admission control (CAC) statistics, use the **clear call admission statistics** command in privileged EXEC mode.

clear call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **clear call admission statistics** command to clear statistics associated with CAC.

Examples

The following example clears the CAC statistics shown in the **show call admission statistics** EXEC command report:

```
Router# show call admission statistics
Total call admission charges: 0, limit 25
Total calls rejected 150, accepted 51
Router# clear call admission statistics
Clear call admission statistics [confirm]y
```

Related Commands

Command	Description
call admission limit	Invokes CAC to scale WAN protocol session limits based on the percentage of system resources being consumed.
call admission load	Configures a CAC metric for scaling WAN protocol session load.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.
show call admission statistics	Monitors the global CAC configuration parameters and the behavior of CAC.

clear ip http client cookie

To remove the HTTP client cookies, use the **clear ip http client cookie** command in privileged EXEC mode.

clear ip http client cookie [**domain** *cookie-domain*| **name** *cookie-name*| **session** *session-name*]

Syntax Description

domain	(Optional) Specifies all cookies in a domain.
cookie-domain	(Optional) Client cookie domain or hostname.
name	(Optional) Specifies cookies matching a specific name.
cookie-name	(Optional) Client cookie name.
session	(Optional) Specifies cookies specific to a client session.
session-name	(Optional) Client session name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to remove the HTTP client cookie named test:

```
Device# clear ip http client cookie name test
```

clear mpf interface

To clear Multi-Processor Forwarding (MPF) packet counts on all physical interfaces, use the clear mpf interface command in user EXEC or privileged EXEC mode.

clear mpf interface

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command has no output. It resets the packet counters shown in the **show mpf interface** command output.

Examples

The following example uses the **clear mpf interface** command to reset the packet counters displayed in the output of the **show mpf interface** command:

```
Router# clear mpf interface
```

Related Commands

Command	Description
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays packet count information on each physical interface.

Command	Description
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

clear mpf punt

To clear Multi-Processor Forwarding (MPF) per-box punt reason and counts, use the **clear mpf punt**command in user EXEC or privileged EXEC mode.

clear mpf punt

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command clears all punt counters and implicitly generates **show mpf punt** output. It resets for each box or router chassis the punt packet counters shown in the **show mpf punt**command output. Packets that are punted are directed for Cisco IOS processing and are not accelerated by MPF.

Examples

The following example clears the type of packets (Type), the reasons for the punt (Message), and the punt packet counts (Count) for the router chassis, then implicitly generates **show mpf punt** output.

```
Router# show mpf punt
  Type      Message         Count
  l2tp      unknown session errors          7
  l2tp      L2TP control          6
  ipv4/verify      adjacency punt          1
  ethernet      unknown ethernet type             542
  ppp      punts due to unknown protocol    333
  arp      ARP request          6
Router# clear mpf punt
        Type              Message                         Count
        arp               ARP request                        38
        ethernet          unknown ethernet type              591
        l2tp              unknown session errors             71790
        l2tp              unsupported output feature         24000
```

The table below describes the fields in the **clear mpf punt** output display.

Table 1: clear mpf punt Field Descriptions

Field	Description
Type	Packet type or encapsulation, such as ARPA, Ethernet, or L2TP.

Field	Description
Message	Reason for the punt of the packet to Cisco IOS processing.
Count	Punt packet count.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
ip mpf	Enables MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

clear ppp subscriber statistics

To clear PPP subscriber statistics and reset counters to zero, use the **clear ppp subscriber statistics**command in privileged EXEC mode.

clear ppp subscriber statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **clear ppp subscriber statistics** command to clear all PPP subscriber statistics and reset counters to zero.

Examples

The following example clears all PPP subscriber statistics and resets counters to zero:

```
Router# clear ppp subscriber statistics
```

Related Commands

Command	Description
show ppp subscriber statistics	Displays PPP statistics.

clear pppatm interface atm

To clear PPP ATM sessions on an ATM interface, use the **clear pppatm interface atm**command in privileged EXEC mode.

clear pppatm interface atm *interface-number*[*sub-interface-number*][**vc**{[[*vpif*]]*vci* |*virtual-circuit-name*}]

Syntax Description

interface-number	ATM interface number.
. *subinterface-number*	(Optional) ATM subinterface number. A period must precede the number.
vc *vpi* / *vci*	(Optional) Specifies virtual circuit (VC) by virtual path identifier (VPI) and virtual channel identifier (VCI). A slash must follow the VPI.
vc *virtual-circuit-name*	(Optional) Specifies VC by name.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command clears the PPP over ATM (PPPoA) sessions in an interface, or in a VC when the VC is specified.

When the **clear pppatm interface atm**command is used to clear sessions on an interface, PPP keepalives continue to work and can be used to detect a broken link.

Examples

The following example clears a PPP ATM session on ATM interface 1/0.10:

```
Router# clear pppatm interface atm 1/0.10
```

Related Commands

Command	Description
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.

Command	Description
show pppatm summary	Displays PPPoA session counts.

clear pppatm statistics

To clear PPP over ATM statistics and reset counters to zero, use the **clear pppatm statistics**command in privileged EXEC mode.

clear pppatm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

Use the **clear pppatm statistics** command to clear PPPoA statistics and reset counters to zero.

Examples

The following example clears PPPoA statistics and reset counters to zero:

```
Router# clear pppatm subscriber statistics
```

Related Commands

Command	Description
show pppatm statistics	Displays PPPoA statistics.

clear pppoe

To clear PPP over Ethernet (PPPoE) sessions, use the **clear pppoe** command in privileged EXEC mode.

clear pppoe {**interface** *type number* [**vc** {[[*vpi/*]] *vci*| **vc-name**}] [**vlan** *vlan-id*]| **rmac** *mac-address* [**sid** *session-id*]| **all**}

Syntax Description

interface *type number*	Interface keyword followed by the interface type and number.
vc *vpi* / *vci*	(Optional) Virtual circuit (VC) keyword followed by a virtual path identifier (VPI), virtual channel identifier (VCI). A slash (/) follows the VPI.
vc-name	(Optional) Name of the VC.
vlan *vlan-id*	(Optional) VLAN identifier.
rmac *mac-address*	(Optional) Remote MAC address.
sid *session-id*	(Optional) Session identifier.
all	(Optional) Specifies that all PPPoE sessions will be cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(2)T	The **vlan** *vlan-id* keyword and argument were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **clear pppoe all** command to clear all PPPoE sessions.

Use the **interface** keyword and arguments and the **vlan** keyword and argument to clear PPPoE sessions on a specific Ethernet 802.1Q VLAN.

Use the **interface**, **vc**, and **vlan** keywords and arguments to clear PPPoE over 802.1Q VLAN sessions on an ATM.

Examples

The following example clears all PPPoE sessions:

```
Router# clear pppoe all
```

clear pppoe derived

To clear the cached PPP over Ethernet (PPPoE) configuration of a PPPoE profile and force the PPPoE profile to reread the configuration from the assigned subscriber profile, use the **clear pppoe derived** command in privileged EXEC mode.

clear pppoe derived group *group-name*

Syntax Description

group *group-name*	PPPoE profile for which the cached PPPoE configuration will be cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A subscriber profile can be configured locally on the router or remotely on an authentication, authorization, and accounting (AAA) server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **clear pppoe derived** command to clear the cached PPPoE configuration of a specified PPPoE profile and force the PPPoE profile to reread the configuration from the assigned subscriber profile.

A subscriber profile contains a list of PPPoE service names. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. You can assign a subscriber profile to a PPPoE profile by using the **service profile** command in BBA group configuration mode.

Examples

The following example clears the cached PPPoE configuration for PPPoE profile "group1". The PPPoE profile will reread the configuration from the subscriber profile that is assigned to that PPPoE profile.

```
Router# clear pppoe derived group1
```

Related Commands

Command	Description
service profile	Assigns a subscriber profile to a PPPoE profile.

Command	Description
show pppoe derived	Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

clear pppoe relay context

To clear the PPP over Ethernet (PPPoE) relay context created for relaying PPPoE Active Discovery (PAD) messages, use the **clear pppoe relay context**command in privileged EXEC mode.

clear pppoe relay context {**all**| **id** *session-id*}

Syntax Description

all	Clears all relay contexts.
id *session-id*	Clears a specific relay context identified in the output of the **show pppoe relay context all**command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to clear relay contexts created for relaying PAD messages.

Examples

The following example clears all PPPoE relay contexts created for relaying PAD messages:

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

Related Commands

Command	Description
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.
show pppoe session	Displays information about currently active PPPoE sessions.

clear pppoe statistics

To clear PPP over Ethernet (PPPoE) statistics and reset counters to zero, use the **clear pppoe statistics**command in privileged EXEC mode.

clear pppoe statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **clear pppoe statistics** command to clear all PPPoE statistic and reset counters to zero.

Examples

The following example clears all PPPoE statistics and resets counters to zero:

```
Router# clear pppoe statistics
```

Related Commands

Command	Description
show pppoe statistics	Displays PPPoE statistics.

connection request username

To specify the username used to authenticate an auto-configuration server (ACS) which makes a connection request to a customer premise equipment (CPE), use the **connection request username**command in TR-069 Agent configuration mode.

connection request username *username*

Syntax Description

username	The user name used to make a connection request to the CPE from the ACS.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows the **connection request username**command when specifying a username:

```
Device(config-cwmp)# connection request username cisco
```

connection request password

To specify the password used to authenticate an auto-configuration server (ACS) which makes a connection request to a customer premise equipment (CPE), use the **connection request password**command in TR-069 Agent configuration mode.

connection request password [*encryption-type*| *cleartext-password*] *passwd*

Syntax Description

encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • 0--Specifies that the text immediately following is not encrypted. • 7--Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
cleartext-password	(Optional) Cleartext Cisco WAN Management Protocol (CWMP) password, which is not encrypted.
passwd	The password that is used in the authentication phase with the ACS and CPE.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to specify the password that is used in the authentication phase. In this example, the password is cisco and is not encrypted:

```
Device(config-cwmp)# connection request password 0 cisco
```

control-packets vlan cos

To set the 802.1P priority bits in 802.1Q frames containing PPP over Ethernet (PPPoE) control packets, use the **control-packets vlan cos** command in BBA group configuration mode. To remove the setting, use the **no** form of this command.

control-packets vlan cos *priority*

no control-packets vlan cos *priority*

Syntax Description

priority	Allows the configuration of VLAN priority bits, for PPPoE control packets. The priority value for PPPoE control packets in the VLAN header can be any number from 0 through 7.

Command Default

No marking is enabled.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

This command allows the setting of class of service (CoS) values on PPPoE control packets to valid priority value compatible with IEEE 802.1P particularly for PPPoEo802.1Q, and PPPoE over QinQ. Settings for PPPoE control packets can differ depending on the BBA group that they are associated with.

Examples

In the following examples, PPPoE control packets associated with BBA group global have a priority of 5, whereas PPPoE control packets associated with BBA group cisco have a priority of 2:

```
Router(config)# bba-group pppoe global
Router(config-bba-group)# control-packets vlan cos
 5
Router(config)# bba-group pppoe cisco
Router(config-bba-group)# control-packets vlan cos
 2
```

The following example shows the setting of 802.1P priority bits in 802.1Q frames containing PPPoE:

```
Router(config-bba-group)# control-packets vlan cos
 5
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

controller shdsl

To configure a controller for single-pair high-bit-rate digital subscriber line (SHDSL) mode, use the **controller shdsl**command in global or controller configuration mode.

Cisco HWIC-4SHDSL and HWIC-2SHDSL

controller shdsl *slot number /subslot number /port number*

Cisco IAD2420 Series

controller shdsl *number*

Syntax Description

number	Controller number. The valid controller number is 0.
slot number	Defines the slot on the router in which the high-speed WAN interface cards (HWIC) is installed.
subslot number	Defines the subslot on the router in which the HWIC is installed.
port number	Defines the port on the router in which the HWIC is installed. By default, Cisco HWIC-4SHDSL and HWIC-2SHDSL use port number 0.

Command Default

Controller number: 0

Command Modes

Cisco HWIC-4SHDSL and HWIC-2SHDSL

Global configuration

Controller configuration

Cisco IAD2420 Series

Global configuration

Command History

Release	Modification
11.3(5)AAA	This command was introduced.
12.2(8)T	This command was implemented on Cisco IAD2420 series IADs.
12.4(15)T	This command was introduced for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router, and on the Cisco 2800 and 3800 series access routers.

Usage Guidelines

This command is used to configure the controller mode and the controller number.

Examples

Examples

The following example uses the controller shdsl command to configure a Cisco HWIC-4SHDSL installed in a Cisco access router, controller number 0, subslot 2, port number 0); the example enters controller configuration mode:

```
Router(config)# controller shdsl 0/2/0
Router(config-controller)#
```

Examples

The following example uses the controller shdsl command to enter SHDSL controller mode on controller number 0; the example also configures ATM mode:

```
Router# controller
 shdsl 0
Router# mode atm
```

Related Commands

Command	Description
show controller shdsl	Displays the controller status and statistics.

cwmp agent

To enable the TR-069 Agent configuration mode, use the **cwmp agent** command in global configuration mode.

cwmp agent

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to enter TR-069 Agent configuration mode:

```
Device(config)# cwmp agent
```

cwmp wan

To define the WAN interfaces on the customer premises equipment (CPE), use the **cwmp wan** command in interface configuration mode.

cwmp wan

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Any interface without this command is considered a LAN interface by TR-069 protocol. There can be multiple WAN and LAN interfaces configured on the CPE. By default, an ATM interface on the CPE will be considered a WAN interface by the TR-069 protocol.

Examples

The following example shows how to define the WAN interfaces on the CPE:

```
Device(config-if)# cwmp wan
```

Related Commands

Command	Description
cwmp wan default	Defines the default WAN interfaces on the CPE.

cwmp wan default

To define the default WAN interfaces on the customer premises equipment (CPE), use the **cwmp wan default**command in interface configuration mode.

cwmp wan default

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Among the multiple WAN interfaces, there can be only one default WAN interface in which the TR-069 communication will happen. If you try to configure this command on multiple interfaces, only the latest configuration will be active and the previous default WAN interface will become a WAN interface, ensuring only one interface is the default at any point in time.

Examples

The following example shows how to define the default WAN interfaces on the CPE:

```
Device(config-if)# cwmp wan default
```

Related Commands

Command	Description
csmp wan	Defines the WAN interfaces on the CPE.

dialer-group

To control access by configuring an interface to belong to a specific dialing group, use the **dialer-group** command in interface configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command.

dialer-group *group-number*

no dialer-group

Syntax Description

group-number	Number of the dialer access group to which the specific interface belongs. This access group is defined with the **dialer-list** command. Acceptable values are nonzero, positive integers between 1 and 10.

Command Default

No access is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

An interface can be associated with a single dialer access group only; multiple **dialer-group** assignment is not allowed. A second dialer access group assignment will override the first. A dialer access group is defined with the **dialer-group** command. The **dialer-list** command associates an access list with a dialer access group.

Packets that match the dialer group specified trigger a connection request.

Examples

The following example specifies dialer access group number 1.

The destination address of the packet is evaluated against the access list specified in the associated **dialer-list** command. If it passes, either a call is initiated (if no connection has already been established) or the idle timer is reset (if a call is currently connected).

```
interface async 1
```

```
 dialer-group 1
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 protocol ip list 101
```

Related Commands

Command	Description
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and an access list.

dialer-list protocol

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** command in global configuration mode. To delete a dialer list, use the **no** form of this command.

dialer-list *dialer-group* **protocol** *protocol-name* {**permit**| **deny**| **list** *access-list-number*| *access-group*}

no dialer-list *dialer-group* [**protocol** *protocol-name* [**list** *access-list-number*| *access-group*]]

Syntax Description

dialer-group	Number of a dialer access group identified in any **dialer-group** interface configuration command.
protocol-name	One of the following protocol keywords: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_router-L1**, **decnet_router-L2**, **decnet_node**, **ip**, **ipx**, **ipv6**, **vines**, or **xns**.
permit	Permits access to an entire protocol.
deny	Denies access to an entire protocol.
list	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
access-list-number	Access list numbers specified in any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types, and IPv6 access lists. See the table below for the supported access list types and numbers.
access-group	Filter list name used in the **clns filter-set** and **clns access-group** commands.

Command Default

No dialer lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
10.3	The following keyword and arguments were added: • list • *access-list-number* and *access-group*
12.2(2)T	The **ipv6** keyword was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The various **no**forms of this command have the following effects:

- The **no dialer-list 1** command deletes all lists configured with list 1, regardless of the keyword previously used (**permit**, **deny**, **protocol**, or **list**).
- The **no dialer-list 1 protocol***protocol-name* commanddeletes all lists configured with list 1 and **protocol** *protocol-name*.
- The **no dialer-list 1 protocol** *protocol-name* **list** *access-list-number*command deletes the specified list.

The **dialer-list protocol** command permits or denies access to an entire protocol. The **dialer-list protocol list**command provides a finer permission granularity and also supports protocols that were not previously supported.

The **dialer-list protocol list** command applies protocol access lists to dialer access groups to control dialing using DDR. The dialer access groups are defined with the **dialer-group**command.

The table below lists the access list types and number range that the **dialer-list protocol list**command supports. The table does not include International Organization for Standardization (ISO) Connectionless Network Services (CLNS) or IPv6 because those protocols use filter names instead of predefined access list numbers.

Table 2: dialer-list protocol Command Supported Access List Types and Number Range

Access List Type	Access List Number Range (Decimal)
AppleTalk	600 to 699
Banyan VINES (standard)	1 to 100
Banyan VINES (extended)	101 to 200
DECnet	300 to 399
IP (standard)	1 to 99
IP (extended)	100 to 199
Novell IPX (standard)	800 to 899
Novell IPX (extended)	900 to 999
Transparent Bridging	200 to 299
XNS	500 to 599

Examples

Dialing occurs when an interesting packet (one that matches access list specifications) needs to be output on an interface. Using the standard access list method, packets can be classified as interesting or uninteresting. In the following example, Integrated Gateway Routing Protocol (IGRP) TCP/IP routing protocol updates are not classified as interesting and do not initiate calls:

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
```

The following example classifies all other IP packets as interesting and permits them to initiate calls:

```
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Then the following command places list 101 into dialer access group 1:

```
dialer-list 1 protocol ip list 101
```

In the following example, DECnet access lists allow any DECnet packets with source area 10 and destination area 20 to trigger calls:

```
access-list 301 permit 10.0 0.1023 10.0 0.1023
access-list 301 permit 10.0 0.1023 20.0 0.1023
```

Then the following command places access list 301 into dialer access group 1:

```
dialer-list 1 protocol decnet list 301
```

In the following example, both IP and VINES access lists are defined. The IP access lists define IGRP packets as uninteresting, but permits all other IP packets to trigger calls. The VINES access lists do not allow Routing Table Protocol (RTP) routing updates to trigger calls, but allow any other data packets to trigger calls.

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
```

```
vines access-list 107 deny RTP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
vines access-list 107 permit IP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
```

Then the following two commands place the IP and VINES access lists into dialer access group 1:

```
dialer-list 1 protocol ip list 101
dialer-list 1 protocol vines list 107
```

In the following example, a CLNS filter is defined and then the filter is placed in dialer access group 1:

```
clns filter-set ddrline permit 47.0004.0001....
!
dialer-list 1 protocol clns list ddrline
```

The following example configures an IPv6 access list named list2 and places the access list in dialer access group 1:

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
!
dialer-list 1 protocol ipv6 list list2
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
clns filter-set	Builds a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
vines access-list	Creates a VINES access list.

dsl enable-training-log

To enable the retrieval of the digital subscriber line (DSL) training log, use the **dsl enable-training-log** command in interface configuration mode. To disable the retrieval of the DSL training log use the **no** form of this command.

dsl enable-training-log [**delay** *seconds* | **ondemand** | [**failure** | **showtime** | [*delay*]]]

no dsl enable-training-log

Syntax Description

delay *seconds*	Delays the retraining, in seconds, of the DSL after the log is retrieved. The range is from 0 to 600.
ondemand	Retrieves the training log from the chipset when the **show dsl atm** command is executed.
failure	Retrieves the training log from the chipset after the line comes out of showtime or when the line fails to synchronize with the digital subscriber line access multiplexer (DSLAM).
showtime	Retrieves the training log from the chipset after the DSL goes into showtime.
delay	Delays the retraining, in seconds, of the DSL after the log is retrieved.

Command Default

The DSL training log is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.

Usage Guidelines

The training log records the events that occur when the router trains or negotiates communication parameters with the DSL access multiplexer (DSLAM). Use this command to enable collection of the DSL logs.

Enabling the training log uses 1 MB of memory. Cisco recommends using the training log for debugging purposes only.

Note Prior to Cisco IOS Release 15.0(1) M, if the DSL training log is configured and a cable is disconnected from the ADSL card and then reconnected, the ADSL interface fails to retrain. To prevent this from happening, disable the DSL training log using the **no dsl enable-training-log** command.

Examples

The following example shows how to enable the training log:

```
Router(config)# interface atm 0/1/0
Router(config-if)# dsl enable-training-log
```

Related Commands

Command	Description
interface atm	Configures an ATM interface.
show dsl interface atm	Displays the DSL line status and training log buffer.

dsl equipment-type

To configure the digital subscriber line (DSL) ATM interface to function as central office or customer premises equipment, use the **dsl equipment-type** command in interface configuration mode. To restore the default equipment type, use the **no** form of this command.

dsl equipment-type {**co**| **cpe**} **ignore-error-duration** *seconds*

no dsl equipment-type

Syntax Description

co	Configures the DSL ATM interface to function as central office equipment.
cpe	Configures the DSL ATM interface to function as customer premises equipment.
ignore-error-duration seconds	Sets the number of seconds for which errors are ignored. The valid range is from 15 to 30. The default is 0.

Command Default

cpe Seconds: 0

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)XL	This command was integrated into Cisco IOS Release 12.2(4)XL on the G.SHDSL WIC on the Cisco 2600 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the G.SHDSL WAN interface card (WIC) on the Cisco 2600 series and Cisco 3600 series routers.
12.2(13)T	The ignore-error-duration keyword was added to interoperate with metalink chipset digital subscriber line access multiplexers (DSLAMs).

Usage Guidelines

This configuration command applies to a specific ATM interface. You must specify the ATM interface before you enter this command.

The ATM interface must be in the shutdown state before you enter this command.

Examples

The following example shows how to configure DSL ATM interface 1/1 to function as central office equipment:

```
Router# configure terminal

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

Router(config-if)# dsl equipment-type co ignore-error-duration 18"“
Router(config-if)# end

Router# clear interface atm
0
/1
```

Related Commands

Command	Description
dsl linerate	Specifies a line rate for the DSL ATM interface.
dsl operating-mode gshdsl	Specifies an operating mode of the DSL ATM interface.

dsl gain-setting rx-offset

To add an offset to the receive (Rx) gain in a modem, use the **dsl gain-setting rx-offset**command in global configuration mode.

dsl gain-setting rx-offset *decimal*

Syntax Description

decimal	Offset (in dB) to the Rx gain. The valid range is from -5 dB to 3 dB, with a granularity of 0.5 dB.

Command Default

0 dB (no offset)

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

In most cases this command does not need to be used because the default value should be adequate. If the service provider improves the line rates, as often happens, using this and other DSL commands will not improve the DSL performance.

Examples

The following example shows how to add an offset of -2 to the receive (Rx) gain of the modem:

```
dsl gain-setting rx-offset -2
```

Related Commands

Command	Description
dsl gain-setting tx-offset	Adds an offset on the Tx gain in the modem and affects the DSP front end.
dsl max-tone-bits	Limits of the number of bits that are loaded into each upstream tone.
dsl noise-margin	Adds an offset on the Rx target noise margin of the modem. The offset is added to the calculated target noise margin.

dsl gain-setting tx-offset

To add an offset to the transmit gain in a modem, use the **dsl gain-setting tx-offset**command in global configuration mode.

dsl gain-setting tx-offset *decimal*

Syntax Description

decimal	Offset (in dB) to the transmit gain. The valid range is from -10 dB to 3 dB, with a granularity of 0.5 dB.

Command Default

0 dB (no offset)

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

In most cases this command does not need to be used because the default value should be adequate. If the service provider improves the line rates, as often happens, using this and other DSL commands will not improve the DSL performance.

Examples

The following example shows how to add an offset of .5 to the transmit (Tx) gain of the modem:

```
dsl gain-setting tx-offset .5
```

Related Commands

Command	Description
dsl gain-setting rx-offset	Adds an offset on the Rx gain in the modem and affects the analog front end.
dsl max-tone-bits	Limits the number of bits that are loaded into each upstream tone.
dsl noise-margin	Adds an offset on the Rx target noise margin of the modem. The offset is added to the calculated target noise margin.

dsl linerate

To specify a line rate for the digital subscriber line (DSL) ATM interface, use the **dsl linerate**command in interface configuration mode. To restore the default line rate, use the **no** form of this command.

dsl linerate {*kbps*| **auto**}

no dsl linerate

Syntax Description

kbps	Line rate, in kilobits per second, for the DSL ATM interface. Allowable entries are **72**, **136**, **200**, **264**, **392**, **520**, **776**, **1032**, **1160**, **1544**, **2056**, and **2312**.
auto	Configures the DSL ATM interface to automatically train for an optimal line rate by negotiating with the far-end digital subscriber line access multiplexer (DSLAM) or WAN interface card (WIC).

Command Default

The DSL ATM interface automatically synchronizes its line rate with the far-end DSLAM or WIC.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)XL	This command was integrated into Cisco IOS Release 12.2(4)XL on the G.SHDSL WIC on the Cisco 2600 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the G.SHDSL WIC on the Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines

This configuration command applies to a specific ATM interface. You must specify the ATM interface before you enter this command.

The ATM interface must be in the shutdown state before you enter this command.

Examples

The following example shows how to configure DSL ATM interface 0/1 to operate at a line rate of 1040 kbps.

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm 0/1

Router(config-if)# dsl linerate 1040
Router(config-if)# end

Router# clear interface atm
0
/
1
```

Related Commands

Command	Description
dsl equipment-type	Configures the DSL ATM interface to function as CO equipment or CPE.
dsl operating-mode gshdsl	Specifies an operating mode of the DSL ATM interface.

dsl lom

To enable LoM monitoring, use the **dsl lom**command in global configuration mode. To disable LOM monitoring, use the **no** form of this command.

dsl lom *number*

no dsl lom

Syntax Description

number	Number of counts after which the router will start retraining.

Command Default

This command is disabled by default. LoM monitoring is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Examples

The following example shows how to enable LoM monitoring with retraining configured for 200 counts:

```
dsl lom 200
```

Related Commands

Command	Description
show dsl interface atm	Displays the ADSL-specific information for a specified ATM interface.

dsl max-tone-bits

To set a limit on the number of bits that are loaded into each upstream tone, use the **dsl max-tone-bits**command in global configuration mode.

dsl max-tone-bits *integer*

Syntax Description

integer	Number of bits that are loaded into each upstream tone. The valid range is from 2 to 14.

Command Default

14 bits per tone, which is the ADSL maximum standard

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

In most cases this command does not need to be used because the default value should be adequate. If the service provider improves the line rates, as often happens, using this and other DSL commands will not improve the DSL performance.

Examples

The following example sets 10 as the maximum number of bits to be loaded into each upstream tone:

```
dsl max-tone-bits 10
```

Related Commands

Command	Description
dsl gain-setting rx-offset	Adds an offset to the Rx gain in the modem and affects the analog front end.
dsl gain-setting tx-offset	Adds an offset on the Tx gain in the modem and affects the DSP front end.
dsl noise-margin	Adds an offset on the Rx target noise margin of the modem. The offset is added to the calculated target noise margin.

dsl noise-margin

To add an offset to the receive (Rx) target noise margin of a modem, use the **dsl noise-margin**command in global configuration mode.

dsl noise-margin *decimal*

Syntax Description

decimal	Offset (in dB) to the Rx target noise margin. The valid range is from -3 dB to -3 dB, with a granularity of 0.5 dB.

Command Default

0 dB (no offset)

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)YN	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

In most cases this command does not need to be used because the default value should be adequate. If the service provider improves the line rates, as often happens, using this and other digital subscriber line (DSL) commands will not improve the DSL performance.

Examples

The following example shows how to add an offset of -0.5 to the noise margin:

```
dsl noise-margin -.5
```

Related Commands

Command	Description
dsl gain-setting rx-offset	Adds an offset on the Rx gain in the modem and affects the analog front end.
dsl gain-setting tx-offset	Adds an offset to the Tx gain in the modem and affects the DSP front end.
dsl max-tone-bits	Limits the number of bits that are loaded into each upstream tone.

dsl operating-mode

To configure the (DSL) operating mode, use the **dsl operating-mode** command in interface configuration mode on Annex A and Annex M interfaces.

dsl operating-mode {**adsl2** [**annex a** | **annex m**] | **adsl2+** [**annex a** | **annex m**] | **ansi-dmt** | **auto** | **itu-dmt**}

The router continues switching between modes, in sequence, until the router reaches the state showtime (which signifies that the connection attempt was successful) and connects using one of the modes. This switching process is designed specifically for expediting DSL performance.

Syntax Description

adsl2	Configures operation in ADSL2 operating mode--ITU G.992.3 Annex A, Annex L, and Annex M. If an Annex operating mode is not chosen, Annex A, Annex L, and Annex M will all be enabled. The final mode will be decided by negotiation with the DSL access multiplexer (DSLAM).
adsl2+	Configures operation in ADSL2+ mode--ITU G.992.5 Annex A and AnnexM. If an Annex A operating mode is not chosen, both Annex and Annex M will be enabled. The final mode will be decided by negotiation with DSLAM.
annex a, m	(Optional) If the annex option is not specified, both Annex A and Annex M will be enabled. The final mode will be decided by negotiation with the Digital Synchronous Line Access Multiplexer (DSLAM).
ansi-dmt	Configures a router to operate in ANSI full-rate mode--ANSI T1.413.
auto	Default setting. Configures the router so that the DSLAM automatically picks the DSL operating mode, in the sequence described in the "Usage Guidelines" section. All supported modes are enabled.
itu-dmt	Configures operation in ITU G.992.1 Annex A full-rate mode.

Command Default

The default is **auto** mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced.
12.2(15)T	This command was implemented on the Cisco 820 series and the Cisco SOHO 70, 76, 77, and 77H platforms.
12.4(11)XJ	This command modification was integrated into the Cisco IOS Release12.4(11)XJ.

Usage Guidelines

In the default auto mode, a router first tries to connect using the configured **ITU** operating modes. If the connection fails, the router tries with **ANSI**/**ETSI** mode for the allowed number of seconds (2 seconds by default). This time can be modified with the **dsl sync interval** command. If this command fails, the router tries **ITU** mode again for the allotted number of seconds (2 seconds by default). The router can be forced to try connecting with ANSI mode first by using the **dsl sync mode ansi** command. If this also fails, the router tries ITU mode again for 3 seconds or the interval specified by dsl sync interval. If that fails, the router repeats the cycle mode, including any modes other than ansi mentioned above.

If the router is forced to connect in a mode other than auto, you must use DSL operating-mode with the attribute auto to set the router back to the default auto mode.

The router continues switching between modes, in sequence as described, until the router reaches the showtime state (which signifies that the connection attempt is successful) and connects, using one of the modes. This switching process is designed specifically for expediting DSL performance.

Examples

The following example shows how to configure Annex M operating mode, using the **dsl operating-mode** command and beginning in interface configuration mode:

```
Router(config-if)# dsl operating-mode adsl2+ annex m
```

dsl operating-mode (ADSL over ISDN)

To specify the operating mode of the digital subscriber line (DSL) for an ATM interface, use the **dsl operating-mode** command in interface configuration mode. To restore the default operating mode, use the **no** form of this command.

dsl operating-mode {**annexb-ur2**| **etsi**| **auto**}

no dsl operating-mode {**annexb-ur2**| **etsi**| **auto**}

Syntax Description

annexb-ur2	Specifies the Deutsche Telekom U-R2 (interface) mode, which transmits and receives ADSL signals according to the ITU-T G.992.1 Annex B standard. This mode supports upstream bins (analog modems) numbered 33 to 53 and downstream bins numbered 64 to 255.
etsi	Specifies Alcatel proprietary ETSI mode, which supports upstream bins numbered 29 to 48 and downstream bins numbered 64 to 255.
auto	Configures a modem to switch between **etsi** mode and **annexb-ur2** mode for connection, following the sequence described in the "Usage Guidelines" section.

Command Default

Mode: **etsi**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced.
12.2(15)T	This command was implemented on the Cisco 820 series and the Cisco SOHO 70, 76, 77, and 77H platforms.

Usage Guidelines

In auto mode, a modem first tries to connect using **etsi** mode. If the connection fails, the modem retries a set number of times. If the modem fails to connect after several retries using **etsi** mode, the modem automatically switches to **annexb-ur2** mode and tries several times to connect using **annexb-ur2** mode. If the modem fails to connect after several retries using **annexb-ur2** mode, the modem automatically switches back to **etsi** mode and tries to connect.

The modem continues switching between modes, in sequence as described, until the modem reaches the state SHOWTIME (which signifies that the connection attempt was successful) and connects using one of the modes. This switching process is designed specifically for expediting DSL modem performance.

Examples

The following example shows how to configure the DSL to operate in **etsi** mode:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm 0
Router(config-if)# dsl operating-mode etsi
Router(config-if)# end
```

Related Commands

Command	Description
show dsl interface atm	Displays information specific to the ADSL for a specified ATM interface.

dsl operating-mode gshdsl

To specify the operating mode of the digital subscriber line (DSL) for an ATM interface, use the **dsl operating-mode** command in interface configuration mode. To restore the default operating mode, use the **no** form of this command.

dsl operating-mode gshdsl symmetric annex {**A**| **B**}

no dsl operating-mode

Syntax Description

symmetric	Configures the DSL ATM interface to operate in symmetrical mode per ITU G.991.2.
annex	Specifies the regional operating parameters.
A	Configures the regional operating parameters for North America. This value is the default.
B	Configures the regional operating parameters for Europe.

Command Default

Region: A

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)XJ	This command was introduced on the Cisco 1700 series routers.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T for the Cisco 1700 series routers.
12.2(4)XL	This command was integrated into Cisco IOS Release 12.2(4)XL for the G.SHDSL WAN interface card (WIC) on the Cisco 2600 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the G.SHDSL WIC on the Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines

This configuration command applies to a specific ATM interface. You must specify the ATM interface before you enter this command.

The ATM interface must be in the shutdown state before you enter this command.

Examples

The following example shows how to configure DSL ATM interface 0/0 to operate in G.SHDSL mode:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm 0/0
Router(config-if)# dsl operating-mode gshdsl symmetric annex
A
Router(config-if)# end

Router# clear interface atm 0/1
```

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

dsl power-cutback

To set the maximum noise margin that can occur on a digital subscriber line (DSL) before a power cutback happens, use the **dsl power-cutback** command in interface configuration mode. To reset the maximum noise margin to the default value of 31, use the **no** form of this command.

dsl power-cutback *dB*

no dsl power-cutback

Syntax Description

dB	Maximum noise margin in decibels. Range is 1 to 30.

Command Default

The maximum noise margin is 31.

Command Modes

Interface configuration

Command History

Release	Modification
12.2T	This command was introduced.

Usage Guidelines

This command is available on ATM interfaces.

Anytime the maximum noise margin is changed by entering the **dsl power-cutback** command, the line will retrain.

Examples

The following example specifies a maximum noise margin of 10 decibels on ATM interface 0:

```
interface ATM 0
 no ip address
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl power-cutback 10
```

dsl-mode shdsl symmetric annex

To specify the operating mode of the digital subscriber line (DSL) controller, use the **dsl-mode shdsl symmetric annex**command in controller configuration mode.

To specify the line coding type of the DSL controller, use the **dsl-mode shdsl symmetric annex coding**command in controller configuration mode. To return the DSL to the default Annex A, use the **no** form of the command.

dsl-mode shdsl symmetric annex mode [**coding type**]

no dsl-mode shdsl symmetric annex mode [**coding type**]

Syntax Description

mode	Sets the DSL operating mode. The valid values are: • **a** : Supports Annex A of the G.991.2 standard for North America. This is the default. • **b** : Supports Annex B of the G.991.2 standard for Europe. • **a-b** : Supports Annex A or B. For CPE mode only. Not supported in CO mode. Selected when the line trains. • **a-b-anfp** : Supports Annex A or B-ANFP. For CPE mode only. Not supported in CO mode. Selected when the line trains. • **b-anfp** : Supports Annex B-ANFP. • f: Supports Annex F, 2-wire mode, line 0 only. • f-g: Supports Annex F-G, 2-wire mode, line 0 only. • g: Supports Annex G, 2-wire mode, line 0 only.
coding	TCPAM line coding.
Type	The valid values are: • 16bit-TCPAM: Sets the line coding to16 bit-TCPAM. • 32bit-TCPAM: Sets the line coding to 32 bit-TCPAM. • AUTO-TCPAM: Detects the central office coding type.

The annex defaults to A for North America.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into the Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	Support for the following additional annex parameters was integrated into Cisco IOS Release 12.3(11)T to support Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series routers: • **b** • **a-b** • **a-b-anfp** • **b-anfp**
12.3(14)T	This command was implemented on Cisco 1800 series routers.
12.4(15)T	Support for the following additional annex parameters was integrated into Cisco IOS Release 12.X(X)T to support Cisco to support Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3700, and Cisco 3800 series routers: • f • f-g • g
12.4(20)T	Support for **coding** *type* parameters was added.

Usage Guidelines

This command is used to configure the DSL controller interface to operate in a specified DSL mode and to set regional operating parameters. The **shdsl** keyword is used to set the mode to SHDSL and configures multirate, high-speed DSL per ITU G.991.2. The **symmetric** keyword configures the controller to symmetric mode. The **annex** keyword configures the controller to use regional operating parameters. The regional operating parameters default to North America. The coding keyword configures the controller Trellis Encoded Pulse Amplitude Modulation (TCPAM) line coding type.

Examples

The following example displays the use of the **controller dsl 0/0**commandto configure the controller in the router configured on the central office (CO) side. Use the **dsl-mode shdsl symmetric annex b**command to configure the controller for multirate, high-speed DSL with symmetric mode for European operating parameters.

```
Router# configure terminal

Router(config)# controller dsl 0/0
Router(config-controller)# line-term co
Router(config-controller)# dsl-mode shdsl symmetric annex b
Router(config-controller)# mode atm
Router(config-controller)#
00:22:07: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to down
Router(config-controller)# line-mode 4-wire
00:23:25: %CONTROLLER-5-UPDOWN: Controller DSL 0/0, changed state to up
00:23:31: %LINK-3-UPDOWN: Interface ATM0/0, changed state to up
00:23:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/0, changed state to up
```

The following example uses the **dsl-mode shdsl symmetric annex command to configure the controller for 2-wire line 0, annex F, AUTO-TCPAM line coding.**

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller dsl 0
Router(config-controller)# line-mode 2-wire line-zero
Router(config-controller)# dsl-mode shdsl symmetric annex f coding ?
 16bit-TCPAM  16bit-TCPAM line coding
 32bit-TCPAM  32bit-TCPAM line coding
 AUTO-TCPAM   AUTO-TCPAM line coding
Router(config-controller)# dsl-mode shdsl symmetric annex f coding auto-tcpam
Router(config-controller)#
Router#
```

Related Commands

Command	Description
controller dsl	Configures the DSL controller.

ip http digest algorithm

To configure the digest algorithm parameter, use the **ip http digest algorithm** command in global configuration mode.

ip http digest algorithm [*digest-algorithm*]

Syntax Description

digest-algorithm	(Optional) The digest algorithm method. The choices for the digest algorithm parameter are MD5 and MD5-sess. MD5 is the default.

Command Default

The digest algorithm parameter is set to MD5.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to change the digest algorithm parameter from MD5 to MD5-sess:

```
Device(config)# ip http digest algorithm md5-sess
```

ip mpf

To enable Multi-Processor Forwarding (MPF) on the second CPU of a Cisco 7200 VXR and Cisco 7301 routers, use the **ip mpf** command in global configuration mode. To disable MPF, use the **no** form of this command.

ip mpf

no ip mpf

Syntax Description

This command has no arguments or keywords.

Command Default

MPF is enabled by default on the second CPU.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XI1	This command was introduced for the Cisco 7301 router.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command allows you to disable and reenable MPF.

MPF is enabled by default on the second CPU (CPU1). The special MPF image is bundled together with the Cisco IOS image and must be purchased.

Note A prerequisite for MPF is that Cisco Express Forwarding (CEF) must be enabled. MPF cannot be enabled unless CEF is enabled first. CEF cannot be disabled (using the **no ip cef** command) unless MPF is disabled first.

Because MPF is enabled by default when the special MPF image is booted up, if CEF is not enabled, MPF is not enabled and boots up with an error message in the error log.

Examples

The following example disables MPF on the second CPU:

```
Router(config)# no ip mpf
```

The following configuration example shows a system where CEF is disabled and the resulting error message showing that MPF cannot be enabled:

```
00:00:13:%MPF-4-NOIPCEF:MPF disabled due to IP CEF disabled
00:00:13:%MPF-6-MODULE:CPU 1 switching module is ready
```

The following configuration example shows that 1) CEF cannot be disabled until MPF is disabled first; and 2) MPF cannot be enabled until CEF is enabled first:

```
Router(config)# no ip cef
%Cannot disable CEF on this platform
Router(config)# no ip mpf
Router(config)# no ip cef
Router(config)# ip mpf
%Can not enable MPF when CEF is disabled.
Router(config)# ip cef
Router(config)# ip mpf
```

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip cef	Enables CEF.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet counter information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets that go through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss *max-segment-size*

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Command Default

The MSS is determined by the originating host.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was modified. This command was changed from **ip adjust-mss** to **ip tcp adjust-mss**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZU2	This command was integrated into Cisco IOS Release 12.2(18)ZU2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When a host (usually a PC) initiates a TCP session with a server, the host negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS size is 1460 bytes, when the default MTU of the containing IP datagram is 1500 bytes.

The PPP over Ethernet (PPPoE) standard supports an MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the Internet Control Message Protocol (ICMP) error messages that must be relayed from the host for path MTU to work.

The **ip tcp adjust-mss** command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The **ip tcp adjust-mss** command is effective only for TCP connections that pass through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value and the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte IP datagram that matches the MTU size of the Ethernet link.

If you are configuring the **ip mtu** command on the same interface as the **ip tcp adjust-mss** command, we recommend that you use the following commands and values:

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

Examples

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
 pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
access-list 101 permit ip 192.168.100.0 0.0.0.255 any
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

logging rate-limit {**number**| **all number**| **console** {**number**| **all number**}} [**except severity**]

no logging rate-limit

Syntax Description

number	Number of messages to be logged per second. Valid values are 1 to 10000. The default is 10.
all	Sets the rate limit for all error and debug messages displayed at the console and printer.
console	Sets the rate limit for error and debug messages displayed at the console.
except *severity*	(Optional) Excludes messages of this severity level and lower. Valid levels are 0 to 7. Severity decreases as the number increases; therefore, severity level 1 indicates a problem more serious than a severity level 3.

Command Default

The default is 10 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.3	This command was integrated into Cisco IOS Release 12.3.
12.3T	This command was integrated into Cisco IOS Release 12.3T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.4T	This command was integrated into Cisco IOS Release 12.4T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **logging rate-limit** command controls the output of messages from the system. Use this command to avoid a flood of output messages. You can select the severity of the output messages and the output rate by using the **logging rate-limit** command. You can issue the **logging rate-limit** command at any time. System performance is not negatively affected and may improve when severities and rates of output messages are specified.

You can use **logging rate-limit** command with or without the **logging synchronous** line configuration command. For example, if you want to see all severity 0, 1, and 2 messages, use the **no logging synchronous** command and specify **logging rate-limit 10 except 2**. By using the two commands together, you cause all messages of 0, 1, and 2 severity to print and limit the less severe ones (higher number than 2) to only 10 per second.

The table below shows the numeric severity level, equivalent meaning in text, and a description for error messages.

Table 3: Error Message Severity Levels, Equivalent Text, and Descriptions

Numeric Severity Level	Equivalent Word	Description
0	**emergencies**	System unusable
1	**alerts**	Immediate action needed
2	**critical**	Critical conditions
3	**errors**	Error conditions
4	**warnings**	Warning conditions
5	**notifications**	Normal but significant condition
6	**informational**	Informational messages only
7	**debugging**	Debugging messages

Cisco 10000 Series Router

To avoid CPU overload and router instability, use the **logging rate-limit** command to limit the rate at which the Cisco 10000 series router logs system messages. To increase the Point-to-Point Protocol call rate, you can turn off console logging completely using the no logging console command.

Examples

The following example shows how to limit message output to 200 per second:

```
Router(config)# logging rate-limit 200
```

Related Commands

Command	Description
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty.
no logging console	Disables syslog message logging to the console terminal.

limit pado service-name

To limit the service-name provided in the PPP over Ethernet Active Discovery Offer (PADO) message to the service-name received in the PPP Protocol over Ethernet Active Discovery Initiation (PADI) message, use the **limit pado service-name** command in BBA group configuration mode. To disable this configuration, use the **no** form of this command.

limit pado service-name

no limit pado service-name

Syntax Description

pado	Limits PADO message capabilities.
service-name	Sends only the requested service name from PADI in the PADO response.

Command Default

All the configured local PPPoE service names are sent in a PADO message.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2SR	This command was introduced.
12.4T	This command was integrated into Cisco IOS release 12.4T.

Usage Guidelines

This command when enabled limits the service-name provided in the PADO message to the service name received in the PADI message, regardless of the number of service name configured for the BBA group.

This command works in conjunction with the **service name match** command.

Examples

In the following example, the service name provided in the PADO message is limited to the service name received in the PADI message:

```
Router(config-bba-group)# limit pado service-name
```

Related Commands

Command	Description
control-packets	Sets the 802.1P priority bits in 802.1Q frames containing PPPoE control packets.

Command	Description
mac-address	Modifies the default MAC address of an interface to a user-defined address.
nas-port-id	Specifies a format for broadband subscriber access line identification coding that complies with a specific set of defined requirements.
pado	Configures PADO delay options.
pppoe	Configures PPPoE server selection.
service	Associates services with this group.
service name match	Forces the PPPoE server to match the service name received in the PADI message from the PPPoE client to a PPPoE service profile from the policy map type service list.
sessions	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 SNMP trap will be generated.
tag	Configures processing options for a tag.
vendor-tag	Sets the PPPoE vendor-specific tag.
virtual-template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

management server password through sessions throttle

management server password

To specify the customer premise equipment (CPE) password that is used in the authentication phase, use the **management server password**command in TR-069 Agent configuration mode.

management server password [*encryption-type*| *cleartext-password*] *passwd*

Syntax Description

encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • 0--Specifies that the text immediately following is not encrypted. • 7--Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
cleartext-password	(Optional) Cleartext Cisco WAN Management Protocol (CWMP) password, which is not encrypted.
passwd	The CPE password that is used in the authentication phase. This password will be provided to the auto-configuration server (ACS) when the CPE is challenged for credential as part of authentication during the session establishment.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

Thefollowing example shows how to specify the CPE password that is used in the authentication phase. In this example, the password is cisco and is not encrypted:

```
Device(config-cwmp)# management server password 0 cisco
```

management server url

To specify the HTTP or HTTPS URL to reach the auto-configuration server (ACS), use the **management server url**command in TR-069 Agent configuration mode.

management server url *acs-url*

Syntax Description

acs-url	The HTTP/HTTPS URL to reach the ACS. This URL is used by the CPE to establish the TR-069 session with the ACS.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows the **management server url**command when specifying an HTTP URL:

```
Device(config-cwmp)# management server url http://172.27.116.78:7547/acs
```

The following example shows the **management server url**command when specifying an HTTPS URL:

```
Device(config-cwmp)# management server url https://172.27.116.78:7547/acs
```

max bandwidth

To specify the total amount of outgoing bandwidth available to switched virtual circuits (SVCs) in the current configuration, use the **max bandwidth**command in interface-ATM-VC configuration mode. To remove the current bandwidth setting, use the **no** form of this command.

max bandwidth *kbps*

no max bandwidth *kbps*

Syntax Description

kbps	Total amount of outgoing bandwidth in kilobits per second available to all SVCs in the current configuration.

Command Default

No default behavior or values

Command Modes

Interface-ATM-VC configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Only the guaranteed cell rate of an SVC is counted toward the maximum bandwidth.

Examples

In following example, an SVC called "svcname" on ATM interface 2/0/0 is configured using the **max bandwidth** command to allow a maximum of 50 Mbps of bandwidth to be used by all of the SVCs in this configuration:

```
interface ATM 2/0/0
 svc svcname
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max bandwidth 50000
```

Related Commands

Command	Description
max vc	Specifies the maximum number of SVCs that can be established using the current configuration.

max vc

To specify the maximum number of switched virtual circuits (SVCs) that can be established using the current configuration, use the **max vc**command in interface-ATM-VC configuration mode. To restore the maximum number of SVCs to the default setting, use the **no** form of this command.

max vc *number*

no max vc *number*

Syntax Description

number	Maximum number of SVCs to be established using the current SVC configuration.

Command Default

4096 SVCs

Command Modes

Interface-ATM-VC configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In following example, an SVC called "svcname" on ATM interface 2/0/0 is configured using the **max vc** command to allow a maximum of 100 SVCs to be established using this configuration:

```
interface ATM 2/0/0
 svc svcname
  encapsulation aal5auto
  protocol ppp virtual-template 1
  max vc 100
```

Related Commands

Command	Description
max bandwidth	Specifies the maximum amount of bandwidth available to all SVCs in the current configuration.
svc	Creates an ATM SVC.

multihop-hostname

To enable a tunnel switch to initiate a tunnel based on the hostname or tunnel ID associated with an ingress tunnel, use the **multihop-hostname** command in VPDN request-dialin subgroup configuration mode. To disable this option, use the **no** form of this command.

multihop-hostname *ingress-tunnel-name*

no multihop-hostname *ingress-tunnel-name*

Syntax Description

ingress-tunnel-name	Network access server (NAS) hostname or ingress tunnel ID.

Command Default

No multihop hostname is configured.

Command Modes

VPDN request-dialin subgroup configuration (config-vpdn-req-in)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 node route processor (NRP).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **multihop-hostname** command only on a device configured as a tunnel switch.

The *ingress-tunnel-name* argument must specify either the hostname of the device initiating the tunnel that is to be to be switched, or the tunnel ID of the ingress tunnel that is to be switched.

Removing the request-dialin subgroup configuration removes the **multihop-hostname** configuration.

Examples

The following example configures a Layer 2 Tunneling Protocol (L2TP) virtual private dialup network (VPDN) group on a tunnel switch to forward ingress sessions from the host named LAC-1 through an outgoing tunnel to IP address 10.3.3.3:

```
vpdn-group 11
 request-dialin
 protocol l2tp
 multihop-hostname LAC-1
 initiate-to ip 10.3.3.3
 local name tunnel-switch
```

Related Commands

Command	Description
dnis	Configures a VPDN group to tunnel calls from the specified DNIS, and supports additional domain names for a specific VPDN group.
domain	Requests that PPP calls from a specific domain name be tunneled, and supports additional domain names for a specific VPDN group.
request-dialin	Creates a request dial-in VPDN subgroup that configures a NAS to request the establishment of a dial-in tunnel to a tunnel server, and enters request dial-in VPDN subgroup configuration mode.
vpdn multihop	Enables VPDN multihop.
vpdn search-order	Specifies how the NAS is to perform VPDN tunnel authorization searches.

nas-port-id format c

To specify a format for broadband subscriber access line identification coding that complies with a specific set of defined requirements, use the **nas-port-id format c** command in BBA group configuration mode. To disable this format implementation, use the **no** form of this command.

nas-port-id format c

no nas-port-id format c

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, the default strings for NAS-Port-ID are used.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
Cisco IOS XE 2.3.0	This command was integrated.

Usage Guidelines

The **nas-port-id format c** command defines 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 guangzhou001/0/31/63/31/127

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 guangzhou001/0/31/63/31/127 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.

Examples

The following example lists the commands for entering BBA group configuration mode and identifying a profile, configuring a virtual template, and specifying format c for the NAS-Port-ID tag:

```
Router(config)# bba-group pppoe bba-pppoeoe
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# nas-port-id format c
!
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and defines a PPPoE profile.
virtual-template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

nas-port format d (bba)

To set the PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format d service, use the **nas-port format d**command in BBA group configuration mode. To remove the extended NAS-Port format, use the **no** form of this command.

nas-port format d *slot* /*adapter* /*port* **[transmit]**

no nas-port format d *slot* /*adapter* /*port*

Syntax Description

slot / *adapter* / *port*	*slot* --Number of bits to store slot number. The range is from 0 to 8. *adapter* --Number of bits to accommodate the adapter value. The range is from 0 to 8. *port* --Number of bits to accommodate the port value. The range is from 0 to 8.
transmit	(Optional) Sends the format to the RADIUS or L2TP Network Server (LNS).

Command Default

If this command is not applied under bba-group mode, the default behavior is to use AAA configured format format d, where *slot* is 4 bits, *adapter* is 1 bit, and *port* is 3 bits.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **nas-port format d**command is applicable only for PPPOE over Ethernet (PPPoEoE) and PPPoE over ATM (PPPoEoA). It does not apply to PPP over ATM (PPPoA). This command can be used if the slot, adapter, and port values are in a different format and need to be changed to the d 4/1/3 format.

Examples

The following example show how to set the PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format d:

```
Router# configure terminal
Router(config)# bba-group pppoe global
Router(config-bba-group)# nas-port format d 2/2/4
```

Related Commands

Command	Description
nas-port-id format c	Specifies a format for broadband subscriber access line identification coding that complies with a specific set of defined requirements.

operating mode

To select an asymmetric digital subscriber line (ADSL) or very high speed digital subscriber line (VDSL) mode of operation, use the operating mode command in controller configuration mode. To restore the default, use the **no** form of this command.

For the 887VA and 887VA-M

operating mode {**auto**| **adsl1**| **adsl2**| **adsl2+**| **vdsl2**| **ansi**}

no operating mode {**auto**| **adsl1**| **adsl2**| **adsl2+**| **vdsl2**| **ansi**}

For the 886VA

operating mode {**auto** [**tone low**]| **adsl1** [**tone low**]| **adsl2** [**tone low**]| **adsl2+** [**tone low**]| **vdsl2**}

no operating mode [**auto** [**tone low**]| **adsl1** [**tone low**]| **adsl2** [**tone low**]| **adsl2+** [**tone low**]| **vdsl2**]

Syntax Description

auto	Trains-up to the mode configured on the digital subscriber line access multiplexer.
adsl1	Configures the router to ADSL1 mode.
adsl2	Configures the router to ADSL2 mode.
adsl2+	Configures the router to ADSL2+ mode.
vdsl2	Configures the router to VDSL2 mode.
ansi	Configures the router to ANSI[1] mode.
tone low	Sets the carrier tone range from 29 to 48, C886VA only.

[1] ANSI = American National Standards Institute

Command Default

auto

Command Modes

Controller configuration

Command History

Release	Modification
15.1(2)T	This command was introduced on the Cisco 886VA.

Usage Guidelines

This command enables customer premise equipment to be manually or automatically configured. It can be manually configured in either ADSL1/2/2+, VDSL2, or ANSI modes. Using the auto mode, the CPE automatically trains-up to the mode configured on the digital subscriber line access multiplexer (DSLAM).

Examples

Note It is recommended to use operating mode auto (default). Using a configuration other than the default configuration for the operating mode can lead to unpredictable behavior on the DSL line.

The following example shows a typical customer premise equipment (CPE) configuration set to auto mode. Outputs in bold are critical. When configured in auto (default), the operating mode command line interface (CLI) is not displayed in the show running command as illustrated in this example.

```
Router# show running
Building configuration...
Current configuration : 1250 bytes
!
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 no ip address
no fair-queue
```

```
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 15/32
  protocol ip 30.0.0.2 broadcast
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

parameter change notify interval

To set the time interval for the parameter change notifications, use the **parameter change notify interval**command in TR-069 Agent configuration mode.

parameter change notify interval *time-interval*

Syntax Description

time-interval	The time interval, in seconds, for the parameter change notifications. The range for the time interval is 15 to 300. The default value is 60.

Command Default

The time interval is 60 seconds.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following shows how to set the time interval for the parameter change notifications to 75 seconds:

```
Device(config-cwmp)# parameter change notify interval 75
```

pppoe-client control-packets vlan cos

To enable class of service (CoS) marking for PPP over Ethernet (PPPoE) control packets on the PPPoE client, use the **pppoe-client control-packets vlan cos** command in either interface configuration mode or ATM virtual circuit configuration mode. To disable CoS marking for PPPoE control packets on the PPPoE client, use the **no** form of this command.

pppoe-client control-packets vlan cos *number*

no pppoe-client control-packets vlan cos *number*

Syntax Description

number	CoS marking value for PPPoE control packets. The range is from 0 to 7. The default is 0.

Command Default

The CoS value is set to 0.

Command Modes

Interface configuration (config-if)

ATM virtual circuit configuration (config-if-atm-vc)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Marking a packet with a CoS value allows you to associate a Layer 2 CoS value with a packet. You can set up to eight different CoS markings.

Examples

The following example shows how to set the CoS marking for PPPoE control packets on the PPPoE client:

```
Router# configure terminal
Router(config)# interface atm0/1/0.1 point-to-point
Router(config-if)# pvc 9/117
Router(config-if-atm-vc)# pppoe-client control-packets vlan cos 2
```

pppoe-client dial-pool-number

To configure a PPP over Ethernet (PPPoE) client and to specify the dial-on-demand routing (DDR) functionality, use the **pppoe-client dial-pool-number** command in interface configuration mode or ATM virtual circuit configuration mode. To disable the configured dial-on-demand functionality, use the **no** form of this command.

pppoe-client dial-pool-number *number* [**dial-on-demand**| **restart** *number*| **service-name** *name*| **mac-override**]

no pppoe-client dial-pool-number *number* [**dial-on-demand**| **restart** *number*| **service-name** *name*| **mac-override**]

Syntax Description

number	A number that is assigned to a configured dialer pool. The range is from 1 to 255.
dial-on-demand	(Optional) Enables the DDR functionality for the PPPoE connection.
restart *number*	(Optional) Allows the timer to be configured in seconds. The range is from 1 to 3600. The default value is 20.
service-name *name*	(Optional) Specifies the service name requested by the PPPoE client. • The service name that allows the PPPoE client to signal a service name to the Broadband Access Aggregation System (BRAS). • By default, no service name is signaled and the service name value is set to NULL.
mac-override	(Optional) Specifies the MAC address to be used as the local MAC address in the corresponding dialer interface when a session is established.

Command Default

A PPPoE client is not configured and the DDR functionality is disabled.

Command Modes

Interface configuration (config-if)

ATM virtual circuit configuration (config-if-atm-vc)

Command History

Release	Modification
12.1(3)XG	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(13)T	This command was modified. The **dial-on-demand** keyword was added to allow the configuration of the DDR interesting traffic control list functionality.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T and the PPPoE client functionality was modified to support multiple clients on a single ATM PVC.
15.2(4)M	This command was modified. The **mac-override** keyword was added.

Usage Guidelines

One PVC supports multiple PPPoE clients, enabling second line connection and redundancy. Use the **pppoe-client dial-pool-number** command to configure one or more concurrent client PPPoE sessions on a single ATM PVC. When a PPPoE session is established in a single PVC, a MAC address that is configured on a dialer interface is used as the local address for multiple PPPoE clients.

Use this command to configure the DDR interesting traffic control list functionality of the dialer interface with a PPPoE client. When the DDR functionality is configured for this command, the following DDR commands must also be configured: **dialer-group**, **dialer hold-queue**, **dialer idle-timeout**, and **dialer-list**.

Tips for Configuring the Dialer Interface

If you are configuring a hard-coded IP address under the dialer interface, you can configure a default IP route using the **ip route** command:

```
ip route 0.0.0.0 0.0.0.0 dialer1
```

But, if you are configuring a negotiated IP address using the **ip address negotiated** command under the dialer interface, you must configure a default IP route using the **ip route** command:

```
ip route 0.0.0.0 0.0.0.0 dialer1 permanent
```

The reason for this configuration is that the dialer interface will lose its IP address when a PPPoE session is brought down (even if the dialer does not go down), and thereby risk removing routes and all IP routes pointed at the dialer interface, including the default IP route. Although the default IP routed back within a minute by IP background processes, you may risk losing incoming packets during the interval.

Examples

The following example shows how to configure multiple PPPoE clients on a single ATM PVC:

```
Device(config)# interface ATM0
Device(config-if)# no ip address
Device(config-if)# no ip mroute-cache
Device(config-if)# no atm ilmi-keepalive
Device(config-if)# pvc 4/20
Device(config-if)# pppoe-client dial-pool-number 1
Device(config-if)# pppoe-client dial-pool-number 2
```

The following example shows how to configure restart time:

```
Device(config)# pppoe-client dial-pool-number 8 restart 80 service-name "test 4"
Device(config)# pppoe-client dial-pool-number 2 dial-on-demand restart 10
```

The following example shows how to configure multiple PPPoE clients on a dialer PVC interface with a configurable MAC address:

```
Device(config)# interface ATM0
Device(config-if)# no ip address
Device(config-if)# no atm ilmi-keepalive
Device(config-if)# pvc 1/32
Device(config-if)# pppoe-client dial-pool-number 2 mac-override
Device(config-if)# pppoe-client dial-pool-number 1 mac-override

Device(config)# interface Dialer1
Device(config-if)# mac-address aaaa.aaaa.aaaa
Device(config-if)# ip address negotiated
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1

Device(config)# interface Dialer2
Device(config-if)# mac-address 0002.0002.0002
Device(config-if)# ip address negotiated
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 2
```

Examples

The following example shows how to configure the PPPoE client DDR idle timer on an Ethernet interface and includes the required DDR commands:

```
Device(config)# vpdn enable
Device(config)# no vpdn logging

Device(config)# vpdn-group 1
Device(config)# request-dialin
Device(config)# protocol pppoe

Device(config)# interface Ethernet1
Device(config-if)# pppoe enable
Device(config-if)# pppoe-client dial-pool-number 1 dial-on-demand

Device(config)# interface Dialer1
Device(config-if)# ip address negotiated
Device(config-if)# ip mtu 1492
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# dialer idle-timeout 180 either
Device(config-if)# dialer hold-queue 100
Device(config-if)# dialer-group 1
Device(config-if)# dialer-list 1 protocol ip permit
```

Examples

The following example shows how to configure the PPPoE client DDR idle timer on an ATM PVC interface and how to include the required DDR commands:

```
Device(config)# vpdn enable
Device(config)# no vpdn logging

Device(config)# vpdn-group 1
Device(config)# request-dialin
Device(config)# protocol pppoe

Device(config)# interface ATM2/0
Device(config-if)# pvc 2/100
Device(config-if)# pppoe-client dial-pool-number 1 dial-on-demand

Device(config)# interface Dialer1
Device(config-if)# ip address negotiated
Device(config-if)# ip mtu 1492
Device(config-if)# encapsulation ppp
Device(config-if)# dialer pool 1
Device(config-if)# dialer idle-timeout 180 either
Device(config-if)# dialer hold-queue 100
Device(config-if)# dialer-group 1
Device(config-if)# dialer-list 1 protocol ip permit
```

Related Commands

Command	Description
debug ppp negotiation	Displays LCP and NCP session negotiations.
debug vpdn pppoe-data	Displays PPPoE session data packets.
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be terminated.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packets	Displays each PPPoE protocol packet exchanged.
dialer-group	Controls access by configuring a virtual access interface to belong to a specific dialing group.
dialer hold-queue	Allows interesting outgoing packets to be queued until a modem connection is established.
dialer idle-timeout	Specifies the idle time before the line is disconnected.
dialer-list	Defines a DDR dialer list to control dialing by a protocol or by a combination of a protocol and an access list.
ip address negotiated	Specifies the IP address for a particular interface that is obtained via PPP/IPCP address negotiation.
ip route	Allows static routes to be established.
show pppoe session	Displays information about currently active PPPoE sessions.

ppp ip address-save aaa-acct-vsa

To enable IPv4 address conservation, use the **ppp ip address-save aaa-acct-vsa** command in global configuration mode. To disable IPv4 address conservation, use the **no** form of this command.

ppp ip address-save aaa-acct-vsa *vsa-string* **password** {*encryption-type address-save-password* | *address-save-password*}

no ppp ip address-save

Syntax Description

vsa-string	Vendor-specific attribute (VSA). The range is 0 to 32 alpha-numeric characters.
password	Specifies the outbound address-save password.
encryption-type	Type of encryption used, if any. • **0—**Specifies that the subsequent text is not encrypted. • **7—**Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
address-save-password	User-configurable Internet Protocol Control Protocol (IPCP) authorization password. The range is 0 to 32 alphanumeric characters.

Command Default

IPv4 address conservation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
Cisco IOS XE Release 3.8S	This command was modified. The **password** keyword was added.

Usage Guidelines

Use this command to enable conservation of IPv4 addresses when a service provider in a dual-stack environment has a limited pool of IPv4 addresses for subscriber allocation. The *vsa-string* argument value is sent to the

RADIUS server, which conserves IPv4 address space by assigning an IPv4 address to a customer premises equipment (CPE) only when needed and releasing it after a defined time interval.

Examples

The following example shows how to configure IPv4 address conservation:

```
Device(config)# ppp ip address-save aaa-acct-vsa cisco password 0 Cisco123
```

ppp ipcp

To configure PPP IP Control Protocol (IPCP) features such as the ability to provide primary and secondary Domain Name Server (DNS) and Windows Internet Naming Service (WINS) server addresses, and the ability to accept any address requested by a peer, use the **ppp ipcp** command in template or interface configuration mode. To disable a PPP IPCP feature, use the no form of this command.

ppp ipcp {**accept-address**| **address** {**accept**| **required**| **unique**}| **dns** {*primary-ip-address* [*secondary-ip-address*] **[aaa] [accept]**| **accept**| **reject**| **request [accept]**}| **header-compression ack**| **ignore-map**| **mask** {*subnet-mask*| **reject**| **request**}| **username unique**| **wins** {*primary-ip-address* [*secondary-ip-address*] **[aaa] [accept]**| **accept**| **reject**| **request [accept]**}}

no ppp ipcp {**accept-address**| **address** {**accept**| **required**| **unique**}| **dns**| **header-compression ack**| **ignore-map**| **mask**| **predictive**| **username unique**| **wins**}

Syntax Description

accept-address	Accepts any nonzero IP address from the peer.
address	Specifies IPCP IP address options: • **accept** --Accepts any nonzero IPv4 or IPv6 address from the peer. • **required** --Disconnects the peer if no IP address is negotiated. • **unique** --Disconnects the peer if the IP address is already in use.
dns	Specifies DNS options: • *primary-ip-address* --IP address of the primary DNS server. • *secondary-ip-address*--(Optional) IP address of the secondary DNS server. • **aaa**--(Optional) Uses DNS data from the AAA server. • **accept**--(Optional) Specifies that any nonzero DNS address will be accepted. • **accept** --Specifies that any nonzero DNS address will be accepted. • **reject** --Rejects the IPCP option if received from the peer. • request--Requests the DNS address from the peer.

header-compression ack	Enables IPCP header compression.
ignore-map	Ignores the dialer map when negotiating the peer IP address.
mask	Specifies IP address mask options: • *subnet-mask* --Specifies the subnet mask to offer the peer. • **reject** --Rejects subnet mask negotiations. • **request** --Requests the subnet mask from the peer.
username unique	Ignores a common username when providing an IP address to the peer.
wins	Specifies WINS options: • *primary-ip-address* --IP address of the primary WINS server. • *secondary-ip-address*--(Optional) IP address of the secondary WINS server. • .**aaa**--(Optional) Use WINS data from the AAA server. • **accept**--(Optional) Specifies that any nonzero WINS address will be accepted. • **accept** --Specifies that any nonzero WINS address will be accepted. • **reject** --Reject the IPCP option if received from the peer. • request--Request the WINS address from the peer.

Command Default

No servers are configured, and no address request is made.

Command Modes

Template configuration Interface configuration (config-if)

Command History

Release	Modification
12.0(6)T	This command was introduced.

Release	Modification
12.1(5)T	This command was modified. The **reject** and **accept**keywords were added.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

Examples

The following examples show use of the **ppp ipcp** command:

```
ppp ipcp accept-address
ppp ipcp dns 10.1.1.3
ppp ipcp dns 10.1.1.3 10.1.1.4
ppp ipcp dns 10.1.1.1 10.1.1.2 accept
ppp ipcp dns accept
ppp ipcp dns reject
ppp ipcp ignore-map
ppp ipcp username unique
ppp ipcp wins 10.1.1.1 10.1.1.2
ppp ipcp wins accept
```

The following examples show how to use the **no** form of the **ppp ipcp** command:

```
no ppp ipcp wins
no ppp ipcp ignore-map
```

Related Commands

Command	Description
debug ppp	Displays information on traffic and exchanges in an internetwork implementing the PPP.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip interfaces	Displays the usability status of interfaces configured for IP.

ppp ipv6cp address unique

To verify if the IPv6 prefix delegation is unique using a PP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated, use the **ppp ipv6cp address unique**command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ppp ipv6cp address unique

no ppp ipv6cp address unique

Syntax Description

This command has no arguments or keywords.

Command Default

Verification of the uniqueness of the IPv6 prefix delegation is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to verify whether the IPv6 prefix delegation is unique using a PPP-enabled interface, and to disconnect the session if the peer IPv6 prefix is duplicated:

```
Router> enable

Router# configure terminal
Router(config)# interface virtual-template 5
Router(config-if)# ppp ipv6cp address unique
```

ppp lcp echo mru verify

To verify the negotiated maximum receive unit (MRU) and adjust the PPP virtual access interface maximum transmission unit (MTU), use the **ppp lcp echo mru verify** command in BBA group configuration mode. To disable the effect of the minimum value, use the **no** form of this command.

ppp lcp echo mru verify [**minimum** *value*]

no ppp lcp echo mru verify [**minimum** *value*]

Syntax Description

minimum	(Optional) Indicates that the value specified is a minimum. If a minimum value is specified, the echo request of that size is sent out on the Link Control Protocol (LCP) connection.
value	(Optional) The minimum echo size sent out on the (LCP) connection. The value can be any integer from 64 to 1500.

Command Default

Timeout on verification requests is the same as the PPP LCP finite state machine (FSM) value.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is entered under the virtual-template interface as a troubleshooting aid to verify the value for the negotiated MRU and to adjust the PPP virtual access interface MTU. The timeout on those verification echo requests would be the same as the PPP LCP FSM timeout. The failure of two such echo requests would be construed as the network not supporting that specific MTU. If a minimum value is configured, echo requests of that alternate size are sent out on the LCP connection. If the minimum value is not configured, or if minimum echo requests also fail, then the PPP session is brought down.

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.

Examples

The following example shows the configuration of two PPPoE profiles:

```
virtual-template 1
 ppp lcp echo mru verify minimum 1200
!
virtual-template 2
 ppp lcp echo mru verify minimum 1200
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and defines a PPPoE profile.
virtual template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

ppp multilink

To enable Multilink PPP (MLP) on an interface and, optionally, to enable Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation, use the **ppp multilink** command in interface configuration mode. To disable Multilink PPP or, optionally, to disable only dynamic bandwidth allocation, use the **no** form of this command.

ppp multilink [bap]

no ppp multilink [**bap [required]**]

Cisco 10000 Series Router

ppp multilink

no ppp multilink

Syntax Description

bap	(Optional) Specifies bandwidth allocation control negotiation and dynamic allocation of bandwidth on a link.
required	(Optional) Enforces mandatory negotiation of BACP for the multilink bundle. The multilink bundle is disconnected if BACP is not negotiated.

Command Default

This command is disabled. When BACP is enabled, the defaults are to accept calls and to set the timeout pending at 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)SX	This command was implemented on the Cisco 10000 series router.
12.2(16)BX	This command was implemented on the ESR-PRE2.
12.2(31)SB 2	This command was integrated into Cisco IOS Release 12.2(31)SB 2.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command applies only to interfaces that use PPP encapsulation.

MLP and PPP reliable links do not work together.

When the **ppp multilink**command is used, the first channel will negotiate the appropriate Network Control Protocol (NCP) layers (such as the IP Control Protocol and IPX Control Protocol), but subsequent links will negotiate only the link control protocol and MLP. NCP layers do not get negotiated on these links, and it is normal to see these layers in a closed state.

This command with the **bap** keyword must be used before configuring any **ppp bap** commands and options. If the **bap required** option is configured and a reject of the options is received, the multilink bundle is torn down.

The **no** form of this command without the **bap** keyword disables both MLP and BACP on the interface.

The **dialer load-threshold** command enables a rotary group to bring up additional links and to add them to a multilink bundle.

Before Cisco IOS Release 11.1, the **dialer-load threshold 1** command kept a multilink bundle of any number of links connected indefinitely, and the **dialer-load threshold 2** command kept a multilink bundle of two links connected indefinitely. If you want a multilink bundle to be connected indefinitely, you must set a very high idle timer.

Note By default, after changing hostnames, an MLP member link does not undergo failure recovery automatically. You must use the **ppp chap hostname** command to define the MLP bundle name on an endpoint. If this command is not configured and the hostname is changed, then a link flap will not return the link back to the bundle.

Cisco 10000 Series Router

The ppp multilink command has no arguments or keywords.

Examples

The following partial example shows how to configure a dialer for MLP:

```
interface Dialer0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 500
 dialer map ip 10.0.0.1 name atlanta broadcast 81012345678901
 dialer load-threshold 30 either
 dialer-group 1
 ppp authentication chap
 ppp multilink
```

Related Commands

Command	Description
compress	Configures compression for LAPB, PPP, and HDLC encapsulations.
dialer fast-idle (interface)	Specifies the idle time before the line is disconnected.

Command	Description
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.
dialer load-threshold	Configures bandwidth on demand by setting the maximum load before the dialer places another call to a destination.
encapsulation ppp	Enables PPP encapsulation.
ppp authentication	Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication is selected on the interface.
ppp bap timeout	Specifies nondefault timeout values for PPP BAP pending actions and responses.
ppp chap hostname	Enables a router calling a collection of routers that do not support this command to configure a common CHAP secret password to use in response to challenges from an unknown peer.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on a MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink mrru	Configures the MRRU value negotiated on an MLP bundle.
ppp multilink slippage	Defines the constraints that set the MLP reorder buffer size.
show ppp bap	Displays the configuration settings and run-time status for a multilink bundle.

ppp multilink fragment disable

To disable packet fragmentation, use the **ppp multilink fragment disable** command in interface configuration mode. To enable fragmentation, use the **no** form of this command.

ppp multilink fragment disable

no ppp multilink fragment disable

Syntax Description

This command has no arguments or keywords.

Command Default

Fragmentation is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp multilink fragmentation**.
12.2	The **no ppp multilink fragmentation** command was changed to **ppp multilink fragment disable**. The **no ppp multilink fragmentation** command was recognized and accepted through Cisco IOS Release 12.2.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

The ppp multilink fragment delay and ppp multilink interleave commands have precedence over the ppp multilink fragment disable command. Therefore, the ppp multilink fragment disable command has no effect if these commands are configured for a multilink interface and the following message displays:

```
Warning: 'ppp multilink fragment disable' or 'ppp multilink fragment maximum' will be
ignored, since multilink interleaving or fragment delay has been configured and have
higher precedence.
```

To completely disable fragmentation, you must do the following:

```
Router(config-if)# no ppp multilink fragment delay
Router(config-if)# no ppp multilink interleave
Router(config-if)# ppp multilink fragment disable
```

Disable multilink fragmentation using the **ppp multilink fragment disable** command if fragmentation causes performance degradation. Performance degradation due to multilink fragmentation has been observed with asynchronous member links.

Examples

The following example disables packet fragmentation:

```
ppp multilink fragment disable
```

Related Commands

Command	Description
ppp multilink fragment delay	Specifies a maximum size, in units of time, for packet fragments on an MLP bundle.
ppp multilink interleave	Enables MLP interleaving.
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink mrru	Configures the Maximum Receive Reconstructed Unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle.

ppp multilink group

To restrict a physical link to join only one designated multilink group interface, use the **ppp multilink group** command in interface configuration mode. To remove this restriction, use the **no** form of this command.

ppp multilink group *group-number*

no ppp multilink group

Syntax Description

group-number	Multilink group number (a nonzero number).

Command Default

If the **ppp multilink group** command is configured on an interface, the interface can join any multilink group. If the **ppp multilink group** command is not configured on an interface, the interface cannot join a multilink group.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0	This command was introduced as the **multilink-group** command on the PRE1 for the Cisco 10000 series router.
12.2	This command was changed to **ppp multilink group**. The **multilink-group** command is accepted by the CLI through Cisco IOS Release 12.2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was implemented on the PRE3 for the Cisco 10000 series router.

Usage Guidelines

When the **ppp multilink group** command is configured on an interface, the interface is restricted from joining any interface but the designated multilink group interface. If a peer at the other end of the interface tries to join a different multilink group, the connection is severed. This restriction applies when Multilink PPP (MLP) is negotiated between the local end and the peer system. The link can still come up as a regular PPP interface.

The **ppp multilink group** command cannot be configured on an interface if the multilink group interface is not configured.

To modify the multilink group configuration on a serial interface, the existing PPP multilink group configuration must be removed from the serial interface.

When the multilink group interface is removed, the PPP multilink group configuration is removed from all the member links that have joined the specified multilink group.

The **ppp multilink group** command is primarily used with the MLP inverse multiplexer as described in the "Configuring Media-Independent PPP and Multilink PPP" chapter in the *Dial Technologies Configuration Guide*.

Cisco 10000 Series Router

The group-number option of the **ppp multilink group** command identifies the multilink group. This number must be identical to the multilink-bundle-number that you assign to a multilink interface. Valid group-number values are:

- MLP over serial-based Link Fragmentation and Interleaving (LFI)
    - 1 to 9999 (Cisco IOS Release 12.2(28)SB and later releases)
    - 1 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)
- Single-VC MLP over ATM-based LFI
    - 10,000 and higher
- Multi-VC MLP over ATM-based LFI
    - 1 to 9999 (Cisco IOS Release 12.2(28)SB and later releases)
    - 1 to 2,147,483,647 (Cisco IOS Release 12.2(31)SB2 and later releases)
- MLP over Frame Relay based LFI
    - 10,000 and higher

Examples

The following example shows how to configure a multilink group interface and configure a serial link to join the multilink group interface:

```
Router(config)# interface multilink 1
Router(config-if)# ip address 192.0.2.1 255.255.255.224
Router(config-if)# encapsulation ppp
Router(config-if)# exit
Router(config)# interface serial 1
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink group 1
Router(config-if)# ppp multilink
Router(config-if)# exit
```

The following sample error message is displayed when a PPP multilink group is configured on a serial link before the multilink group interface is configured:

```
Router(config)# interface serial 2
Router(config-if)# ppp multilink group 1
% Multilink group interface does not exist. Please create a group interface first
```

The following sample error message is displayed when the multilink group configuration on a serial link is modified before the existing multilink group configuration is removed:

```
Router# show running-config interface serial4/0

Building configuration...

Current configuration : 188 bytes
!
interface Serial4/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
Router# configure terminal
Router(config)# interface serial4/0
Router(config-if)# ppp multilink group 4
% Link is already part of Multilink1 group interface. Please detach it from the group
interface first.
```

The following sample output displays the serial interface configuration before and after the removal of the multilink group interface:

```
Router# show running-config interface serial5/0

Building configuration...
Current configuration : 188 bytes
!
interface Serial5/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
Router# configure terminal
Router(config)# no interface Multilink 1
% Please 'shutdown' this interface before trying to delete it
Router(config)# interface Multilink 1
Router(config-if)# shutdown
Router(config-if)#
*Aug  2 17:35:11.825: %LINK-5-CHANGED: Interface Multilink1, changed state to administratively
 down
*Aug  2 17:35:11.826: %LINEPROTO-5-UPDOWN: Line protocol on Interface Multilink1, changed
state to down
*Aug  2 17:35:11.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0, changed
state to down
*Aug  2 17:35:11.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0, changed
state to down
Router(config-if)# exit
Router(config)#
*Aug  2 17:35:15.908: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial5/0, changed
state to up
*Aug  2 17:35:15.908: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0, changed
state to up
Router(config)# no interface Multilink1
% The multilink group configuration will be removed from all the member links.
!
Router# show running-config interface serial5/0

Building configuration...
Current configuration : 165 bytes
!
interface Serial5/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink fragment size 1000
 ppp multilink mrru local 1524
 serial restart-delay 0
end
```

Related Commands

Command	Description
encapsulation ppp	Enables PPP encapsulation on a serial interface.

Command	Description
interface multilink	Creates a multilink bundle or enters multilink interface configuration mode.
ip address	Configures an IP address for an interface.
ppp multilink	Enables an MLP on an interface.

ppp ncp override local

To track attributes received in authorization from RADIUS, verify the permitted Network Control Program (NCP), reject the current NCP negotiation, and override the local dual-stack configuration, use the **ppp ncp override local**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ppp ncp override local

no ppp ncp override local

Syntax Description

This command has no arguments or keywords.

Command Default

The tracking of attributes from RADIUS and the local configuration override are not enabled. The local configuration is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Framed attributes are primarily used for address allocation. The RADIUS server maintains a pool of both IPv4 addresses and IPv6 prefixes. If IPv4 address or IPv6 prefix attributes are absent in the access-accept response from RADIUS, the **ppp ncp override local** command can be used to override local configuration.

Examples

The following example shows how to override the local IPv6 or IPv4 dual-stack configuration:

```
Router> enable

Router# configure terminal
Router(config)# ppp ncp override local
```

ppp timeout ncp

To set a time limit for the successful negotiation of at least one network layer protocol after a PPP connection is established, use the **ppp timeout ncp**command in interface configuration mode. To remove the time limit, use the **no** form of this command.

ppp timeout ncp *seconds*

no ppp timeout ncp

Syntax Description

seconds	Maximum time, in seconds, PPP should wait for negotiation of a network layer protocol. If no network protocol is negotiated in the given time, the connection is disconnected.

Command Default

No time limit is imposed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced as **ppp negotiation-timeout**.
12.2	This command was changed to **ppp timeout ncp**. The **ppp negotiation-timeout**command was accepted by the command line interpreter through Cisco IOS Release 12.2.
Cisco IOS XE Release 3.2S	Support for IPv6 was added.

Usage Guidelines

The **ppp timeout ncp** command protects against the establishment of links that are physically up and carrying traffic at the link level, but are unusable for carrying data traffic due to failure to negotiate the capability to transport any network level data. This command is particularly useful for dialed connections, where it is usually undesirable to leave a telephone circuit active when it cannot carry network traffic.

Examples

The following example sets the Network Control Protocol (NCP) timer to 8 seconds:

```
ppp timeout ncp 8
```

Related Commands

Command	Description
absolute-timeout	Sets the interval for closing user connections on a specific line or port.
dialer idle-timeout (interface)	Specifies the idle time before the line is disconnected.

ppp unique address accept-access

To track duplicate addresses received from RADIUS and create a standalone database, use the **ppp unique address accept-access**command in global configuration mode. To disable this feature and remove the database, use the **no** form of this command.

ppp unique address accept-access

no ppp unique address accept-access

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The ppp unique address accept-access command enables the IPv6 router to track and check duplicate attributes received in an Access-Accept response from RADIUS, and triggers creation of a new, standalone database that contains the Access-Accept responses received since the feature was enabled.

The following RADIUS attributes are tracked in this database and checked when an Access-Accept response is received:

- Framed-IP-Address
- Framed-IPv6-Prefix
- Delegated-IPv6-Prefix

All of these RADIUS attributes from this list are checked against the database for duplicates and, if none are found, added to the database exactly as presented in the RADIUS attribute.

Examples

The following example enables this feature:

```
Router (config)# ppp unique address accept-access
```

pppoe enable

To enable PPP over Ethernet (PPPoE) sessions on an Ethernet interface or subinterface, use the **pppoe enable** command in the appropriate configuration mode. To disable PPPoE, use the **no** form of this command.

pppoe enable [**group** *group-name*]

no pppoe enable

Syntax Description

group	(Optional) Specifies a PPPoE profile to be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Command Default

PPPoE is disabled by default.

Command Modes

Interface configuration (config-if)

Subinterface configuration (config-subif)

VLAN configuration (vlan)

VLAN range configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(5)T	This command was modified to enable PPPoE on IEEE 802.1Q encapsulated VLAN interfaces.
12.2(15)T	The **group** keyword and the *group-name* argument were added.
12.3(2)T	This command was implemented in VLAN configuration mode and VLAN range configuration mode.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was implemented on the Cisco 10000 series routers.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

- If a PPPoE profile is not specified by using the **group** option, PPPoE sessions will be established using values from the global PPPoE profile.
- PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

Examples

The following example shows how to enable PPoE sessions on Ethernet interface 1/0. PPPoE sessions are established using the PPPoE parameters in the global PPPoE profile.

```
Device(config)# interface ethernet 1/0
Device(config-if)# pppoe enable
Device(config-if)# bba-group pppoe global
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# sessions max limit 8000
Device(config-bba-group)# sessions per-vc limit 8
Device(config-bba-group)# sessions per-mac limit 2
```

Examples

The following example shows how to enable PPPoE on an 802.1Q VLAN subinterface. PPPoE sessions are established using the PPPoE parameters in PPPoE profile vpn1.

```
Device(config)# interface ethernet 2/3.1
Device(config-subif)# encapsulation dot1Q 1
Device(config-subif)# pppoe enable group vpn1
Device(config-subif)# bba-group pppoe vpn1
Device(config-bba-group)# virtual-template 1
Device(config-bba-group)# sessions per-vc limit 2
Device(config-bba-group)# sessions per-mac limit 1
```

Examples

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

```
Device(config)# interface fastethernet 0/0
Device(config-if)# no ip address
Device(config-if)# no ip mroute-cache
Device(config-if)# duplex half
Device(config-if)# vlan-range dot1q 20 30
Device(config-if-vlan-range)# pppoe enable group PPPOE
Device(config-if-vlan-range)# exit-vlan-config
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.

Command	Description
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a device and sets the PPPoE session-count threshold.
sessions per-vlan limit	Specifies the maximum number of PPPoE sessions in each VLAN.

pppoe limit max-sessions

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

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, use the **pppoe limit max-sessions**command in VPDN group configuration mode. To remove this specification, use the **no** form of this command.

pppoe limit max-sessions *number-of-sessions* [**threshold-sessions** *number-of-sessions*]

no pppoe limit max-sessions

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the maximum number of interfaces on the router.
threshold-sessions	(Optional) Sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the maximum number of interfaces on the router.

Command Default

The maximum number of sessions is not set.

Command Modes

VPDN group configuration (config-vpdn)

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was replaced by the **sessions max limit** command.

Usage Guidelines

PPPoE session limits configured using the **pppoe limit per-vc**, **pppoe limit per-vlan**, **pppoe max-sessions**, **pppoe max-sessions** (VC), and **pppoe max-sessions**(subinterface) commands take precedence over limits configured for the router using the **pppoe limit max-sessions** command.

Examples

The following example shows a limit of 100 PPPoE sessions configured for the router:

```
vpdn enable
vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
 pppoe limit max-sessions 100
```

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

pppoe limit per-mac

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-mac** command is replaced by the **sessions per-mac limit** command. See the **sessions per-mac limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions to be sourced from a MAC address, use the **pppoe limit per-mac** command in VPDN configuration mode.

pppoe limit per-mac *number*

Syntax Description

number	Maximum number of PPPoE sessions that can be sourced from a MAC address.

Command Default

100 sessions

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-mac limit** command.

Examples

The following example sets a limit of 10 sessions to be sourced from a MAC address:

```
pppoe limit per-mac 10
```

Related Commands

Command	Description
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit per-vc

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-vc** command is replaced by the **sessions per-vc limit**command. See the **sessions per-vc limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions to be established over a virtual circuit (VC), use the **pppoe limit per-vc** command in VPDN configuration mode.

pppoe limit per-vc *number*

Syntax Description

number	Maximum number of PPPoE sessions that can be established over an ATM PVC.

Command Default

100 sessions

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-vc limit** command.

Examples

The following example sets a limit of 10 sessions to be established over a VC:

```
pppoe limit per-vc 10
```

Related Commands

Command	Description
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions under each VLAN.

pppoe limit per-vlan

Note Effective with Cisco IOS Release 12.2(28)SB, the **pppoe limit per-vlan** command is replaced by the **sessions per-vlan limit** command. See the **sessions per-vlan limit** command for more information.

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted under each virtual LAN (VLAN), use the **pppoe limit per-vlan**command in VPDN configuration mode. To remove this specification, use the **no** form of this command.

pppoe limit per-vlan *number*

no pppoe limit per-vlan

Syntax Description

number	Maximum number of PPP over Ethernet sessions permitted under each VLAN.

Command Default

100 PPPoE sessions per VLAN

Command Modes

VPDN configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was replaced by the **sessions per-vlan limit** command.

Usage Guidelines

If the **pppoe max-session** command is configured on a VLAN, that command will take precedence over the **pppoe limit per-vlan** command. The **pppoe limit per-vlan** command applies to all VLANs on which the **pppoe max-session** command has not been configured.

The **pppoe limit per-vlan** command must be configured after the accept dial-in VPDN group has been configured using the **accept-dialin** VPDN configuration command.

Examples

The following example shows a maximum of 200 PPPoE sessions configured for an 802.1Q VLAN subinterface:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 pppoe enable
!
vpdn enable
vpdn-group 1
```

```
accept dialin
 protocol pppoe
 virtual-template 1
pppoe limit per-vlan 200
```

Related Commands

Command	Description
accept dial-in	Creates an accept dial-in VPDN subgroup.
debug vpdn pppoe-data	Displays data packets of PPPoE sessions.
debug vpdn pppoe-error	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packet	Displays each PPPoE protocol packet exchanged.
pppoe enable	Enables PPPoE sessions on an Ethernet interface.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions to be established over a VC.
pppoe max-sessions	Specifies the maximum number of PPPoE sessions permitted under a VLAN.

pppoe max-sessions

To specify the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on an ATM permanent virtual circuit (PVC), PVC range, virtual circuit (VC) class, or Ethernet subinterface, use the **pppoe max-sessions** command in the appropriate mode. To remove this specification, use the **no** form of this command.

pppoe max-sessions *number-of-sessions* [**threshold-sessions** *number-of-sessions*]

no pppoe max-sessions

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted. The PPPoE sessions range depends on the device that you use. The range is 1 to 31992 on a Cisco 7200 series device. **Note** The PPPoE session limit in the case of a PVC range applies to *each* PVC in the range. This limit is not cumulative on *all* PVCs belonging to the range.
threshold-sessions	(Optional) Sets the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The PPPoE sessions range depends on the device that you use. The range is 8500 to the maximum number specified for the PPPoE sessions on a Cisco 7200 series device.

Command Default

The maximum number of sessions is not set.

Command Modes

ATM PVC range configuration (config-if-atm-range) ATM PVC-in-range configuration (config-if-atm-range-pvc) ATM VC-class configuration (config-vc-class) Ethernet subinterface configuration (config-if) Interface-ATM-VC configuration (config-if-atm-vc)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(4)T	This command was modified to limit PPPoE sessions on ATM PVCs, PVC ranges, and VC classes.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC for Ethernet interfaces on the Cisco 7600 SIP-400.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

PPPoE sessions can be limited in the following ways:

- The **pppoe limit max-sessions**command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.

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

- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.
- The **pppoe limit per-vc** and **pppoe limit per-vlan**commands limit the number of PPPoE sessions on all PVCs or VLANs on the router.
- The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc**and **pppoe limit per-vlan**commands.

PPPoE session limits created on an ATM PVC take precedence over limits created in a VC class or ATM PVC range.

Examples

Examples

The following example shows a limit of 200 PPPoE sessions configured for the subinterface:

```
interface FastEthernet 0/0.10
 encapsulation dot1Q 10
 pppoe enable
 pppoe max-sessions 200
```

Examples

The following example shows a limit of 10 PPPoE sessions configured for the PVC:

```
interface ATM1/0.102 multipoint
 pvc 3/304
 encapsulation aal5snap
 protocol pppoe
 pppoe max-sessions 10
```

Examples

The following example shows a limit of 20 PPPoE sessions that will be permitted per PVC in the VC class called "main":

```
vc-class atm main
 pppoe max-sessions 20
```

Examples

The following example shows a limit of 30 PPPoE sessions that will be permitted per PVC in the PVC range called "range-1":

```
interface atm 6/0.110 multipoint
 range range-1 pvc 100 4/199
 encapsulation aal5snap
 protocol ppp virtual-template 2
 pppoe max-sessions 30
```

Examples

The following example shows a limit of 10 PPPoE sessions configured for "pvc1", which is part of the ATM PVC range called "range1":

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

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
pppoe limit max-sessions	Specifies the maximum number of PPPoE sessions permitted on a router.
pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
sessions max limit	Specifies the maximum number of PPPoE sessions permitted on a router.

pppoe server circuit-id delay

To specify the delay based on the PPP over Ethernet (PPPoE) tag circuit ID client, use the**pppoe server circuit-id delay** command in BBA group configuration mode. To remove the delay, use the **no** form of this command.

pppoe server circuit-id delay *milliseconds* **string [contains]** *circuit-id-string*

no pppoe server circuit-id delay *milliseconds* **string [contains]** *circuit-id-string*

Syntax Description

milliseconds	Time in milliseconds for PPPoE Active Discovery Offer (PADO) delay. The time range is between 0 to 9999 milliseconds.
string	Specifies the circuit ID string.
contains	Specifies the partial string match that contains the remote ID string.
circuit-id-string	Circuit ID tag sent by Digital Subscriber Line Access Multiplexer (DSLAM) or the client in the PPPoE Active Discovery Initiation (PADI) packet. **Note** The value for the *circuit-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, circuit ATM1/ 0/ 0 VC 0/100).

Command Default

If no PADO delay is defined or matched, the PADO is transmitted without delay.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB3	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.0(1)M	This command was integrated into Cisco IOS 15.0(1)M.

Usage Guidelines

Use the **pppoe server circuit-id delay** command to configure a PADO transmission delay per circuit ID. The PPPoE Smart Server Selection feature allows you to configure a specific PADO delay for a received PADI packet. The PADO delay establishes the order in which the Broadband Remote Access Servers (BRASs) respond to PADIs by delaying their responses to particular PADIs as per the delay time specified.

Examples

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

```
Router(config)# bba-group pppoe name1
Router(config-bba-group)# pppoe server circuit-id delay 20 string contains TEST

Router(config-bba-group)# pppoe server circuit-id delay 10 string XTH

Router(config-bba-group)# pppoe server circuit-id delay 30 string contains XTH-TEST

Router(config-bba-group)# pado delay 50
```

Generally, the first match found in the list is considered for the delay value. If the remote ID in the client PPPoE tag contains XTH-TEST, then the delay value is 20. In this case, the first match succeeds and the configuration never reaches a delay of 30. If the remote ID in the client PPPoE tag contains TH-no, then no match is found.

The following example shows how to match the circuit ATM1/ 0/ 0 VC 0/100 string by using a circuit ID or remote ID delay configured for the PPPoE server:

```
Router(config)# bba-group pppoe server-selection
Router(config-bba-group)# pppoe server circuit-id delay 45 string "circuit ATM1/0/0 VC
0/100"
Router(config-bba-group)# pado delay circuit-id 35
Router(config-bba-group)# pado delay 45
```

The following examples show the PADO delay configurations using circuit ID:

1. If the PADI has a circuit ID and a remote ID tag, and the BBA group on the server does not have a circuit ID or remote ID (matching or non-matching) configured, the value configured via **pado delay** *delay-value* is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1. If the PADI has a circuit ID tag and the BBA group on the server has a circuit ID configured, but they do not match, the value configured via **pado delay circuit-id** *delay-value*is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 2222 string Ethernet1/0:T
Router(config-bba-group)#pppoe server circuit-id string contains TT
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1 If the BBA group on the server has a matching circuit ID configured (partial or strict), the per-circuit-id delay which is configured using the **delay** argument in the **pppoe server circuit-id delay** *value* string *circuit-id-string* command*:*

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 5555 string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1 If the BBA group on the server has a matching circuit ID configured (partial or strict), and no delay value is configured for the circuit ID string, the PADO delay value configured with the **pado delay circuit-id** *delay-value* command is used.

Server example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1 If the delay value is configured as zero and "nvgen" is the delay string, the non-volatile generation (NVGEN) process is not executed on the delay string, only if you have not configured the delay while configuring the circuit ID.

2 If you configure both the partial and strict match strings for a circuit ID, the preference depends on the order in which they are encountered:

Server example:

```
Router(config)#bba-group pppoe 1
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#vendor-tag remote-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 2222 string contains S
Router(config-bba-group)#pppoe server circuit-id delay 4444 string Ethernet1/0:S
```

Client example:

```
Router(config)#bba-group pppoe global
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#test vendor-tag circuit-id string S
```

1 In the case of remote ID configurations, the behavior is the same as described earlier for circuit IDs. If both the remote ID and circuit ID are configured, preference is given to the circuit ID configuration.

2 If the PADO delay is found to be the maximum allowed value (9999 msec), the PADI is discarded as shown in the example:

```
Router(config)#bba-group pppoe 1
Router(config-bba-group)#virtual-template 1
Router(config-bba-group)#vendor-tag circuit-id service
Router(config-bba-group)#vendor-tag remote-id service
Router(config-bba-group)#pado delay 3333
Router(config-bba-group)#pado delay circuit-id 1111
Router(config-bba-group)#pppoe server circuit-id delay 9999 string contains S
Router(config)#end
Router#show debug
PPPoE:
  PPPoE protocol events debugging is on
  PPPoE protocol errors debugging is on
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
pado delay	Establishes the order in which the BRASs respond to PADIs by delaying their responses to particular PADIs as per the delay time specified.
pppoe server remote-id delay	Specifies the delay based on the PPPoE tag remote ID client.
virtual template	Configures a PPPoE profile with a virtual template to be used for cloning virtual access interfaces.

pppoe server remote-id delay

To specify the delay to be applied on the PPP over Ethernet (PPPoE) tag remote ID client, use the **pppoe server remote-id delay** command in BBA group configuration mode. To remove the delay, use the **no** form of this command.

pppoe server remote-id delay *milliseconds* **string [contains]** *remote-id-string*

no pppoe server remote-id delay *milliseconds* **string [contains]** *remote-id-string*

Syntax Description

milliseconds	Time in milliseconds for the PPPoE Active Discovery Offer (PADO) delay.
string	Specifies the remote ID string.
contains	(Optional) Specifies the partial string match that contains the remote ID string.
remote-id-string	Remote ID tag sent by Digital Subscriber Line Access Multiplexer (DSLAM) or the client in the PPPoE Active Discovery Initiation (PADI) packet. **Note** The value for the *remote-id-string*argumentcan contain spaces when enclosed with double quotation marks (for example, subscr mac 1111.2222.3333).

Command Default

If no PADO delay is defined or matched, the PADO is transmitted without delay.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB3	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS Release XE 2.4.
15.0(1)M	This command was integrated.

Usage Guidelines

The PPPoE Smart Server Selection feature allows you to configure a specific PADO delay for a received PADI packet. The PADO delay establishes the order in which the Broadband Remote Access Servers (BRASs) respond to PADIs by delaying their responses to particular PADIs by various times.

Use the **pppoe server remote-id delay** command to configure a PADO transmission delay per remote ID.

Examples

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

```
Router(config)# bba-group pppoe name1
Router(config-bba-group)# pppoe server remote-id delay 20 string contains TEST

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

Router(config-bba-group)# pado delay 50
```

Generally, the first match found in the list is considered for the delay value. If the remote ID in the client PPPoE tag contains XTH-TEST, then the delay value is 20. In this case, the first match succeeds and the configuration never reaches a delay of 30. If the remote ID in the client PPPoE tag contains TH-no, then no match is found.

The following example shows how to match the subscr mac 1111.2222.3333 string by using a remote ID delay configured for PPPoE server:

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

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
pppoe server circuit-id delay	Specifies the delay based on the PPPoE tag circuit ID client.

pppoe service

To add a PPP over Ethernet (PPPoE) service name to a local subscriber profile, use the **pppoe service** command in subscriber profile configuration mode. To remove a PPPoE service name from a subscriber profile, use the **no** form of this command.

pppoe service *service-name*

no pppoe service *service-name*

Syntax Description

service-name	Name of the PPPoE service to be added to the subscriber profile.

Command Default

A PPPoE service name is not part of a subscriber profile.

Command Modes

Subscriber profile configuration (config-sss-profile)#

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

A subscriber profile contains a list of PPPoE service names. Use the **pppoe service** command to add PPPoE service names to a local subscriber profile.

When you configure PPPoE service selection, you define a RADIUS service profile for each service name, list the service names that you want to advertise in a subscriber profile, and then assign the subscriber profile to a PPPoE profile. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

Examples

The following example shows PPPoE service names being added to the subscriber profile called "listA":

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default local
!
! Configure the subscriber profile
subscriber profile  listA
 pppoe service isp1
 pppoe service isp2
 pppoe service isp3
!
! Configure the PPPoE profile
bba-group pppoe group1
 virtual-template 1
 sessions per-vc  5
 service profile listA
!
! Attach the PPPoE profile to a PVC
interface atm1/0.1
 pvc 2/200
 protocol PPPoE group1
!
```

Related Commands

Command	Description
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
show pppoe derived	Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

pppoe-sessions threshold

To configure the per-physical interface threshold value of the Cisco ASR 1000 Series Aggregation Services Routers, use the **pppoe-sessions threshold**command in interface configuration mode. To disable the threshold value, use the **no** form of this command.

pppoe-sessions threshold *number*

no pppoe-sessions threshold *number*

Syntax Description

number	Maximum number of permissible PPPoE sessions. Range: 1 to 65535.

Command Default

The per-physical interface threshold value is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to configure 90 PPPoE sessions as the per-physical threshold value on the Cisco ASR 1000 Series Router:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0
Router(config-if)# pppoe-sessions threshold 90
```

Related Commands

Command	Description
sessions threshold	Configures the global threshold value of the PPPoE session on the Cisco ASR1000 Series Router.

protocol pppoe (ATM VC)

To enable PPP over Ethernet (PPPoE) sessions to be established on permanent virtual circuits (PVCs), use the **protocol pppoe** command in the appropriate configuration mode. To disable PPPoE, use the **no** form of this command.

protocol pppoe [**group** *group-name*| **global**]

no protocol pppoe [**group** *group-name*| **global**]

Syntax Description

group	(Optional) Specifies a PPPoE profile to be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.
global	(Optional) Specifies a global PPPoE profile to be used by PPPoE sessions on the interface.

Command Default

PPPoE is not enabled.

Command Modes

ATM PVC-in-range configuration (cfg-if-atm-range-pvc) ATM PVC range configuration (config-if-atm-range) ATM VC class configuration (config-vc-class) ATM VC configuration (config-if-atm-vc)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

If a PPPoE profile is not specified by using the **group**option, PPPoE sessions will be established using values from the global PPPoE profile. PPPoE profiles must be configured using the **bba-group pppoe** command.

Examples

The following example shows PPPoE configured in virtual circuit (VC) class "class-pppoe-global" and on the range of PVCs from 100 to 109. PVCs that use VC class "class-pppoe-global" will establish PPPoE sessions using the parameters configured in the global PPPoE profile. PVCs in the PVC range will use PPPoE parameters defined in PPPoE profile "vpn1".

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000
 sessions per-vc limit 8
 sessions per-mac limit 2
!
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
vc-class atm class-pppoe-global
 protocol pppoe
!
interface ATM1/0.10 multipoint
 range range-pppoe-1 pvc 100 109
  protocol pppoe group vpn1
 !
interface ATM1/0.20 multipoint
 class-int class-pppoe-global
 pvc 0/200
!
 pvc 0/201
 !
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
debug pppoe	Displays debugging information for PPPoE sessions.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC and sets the PPPoE session-count threshold.

protocol pppovlan dot1q

To configure an ATM PVC to support PPPoE over a specific IEEE 802.1Q VLAN or range of VLANs, use the **protocol pppovlan dot1q** command in ATM VC configuration or VC class configuration mode. To disable ATM PVC support for PPPoE for a specific IEEE 802.1Q VLAN or a range of VLANs, use the **no** form of this command.

protocol pppovlan dot1q {*vlan-id*| *start-vlan-id end-vlan-id*} [**group** *group-name*]

no protocol pppovlan dot1q {*vlan-id*| *start-vlan-id end-vlan-id*} [**group** *group-name*]

Syntax Description

vlan-id	VLAN identifier. Valid values range from 1 to 4095.
start-vlan-id	VLAN identifier of the first VLAN in the range. Valid values range from 1 to 4095.
end-vlan-id	VLAN identifier of the last VLAN in the range. Valid values range from 1 to 4095.
group	(Optional) Specifies that a PPPoE profile will be used by PPPoE sessions on the interface.
group-name	(Optional) Name of the PPPoE profile to be used by PPPoE sessions on the interface.

Command Default

ATM PVC support for PPPoE over 802.1Q VLAN encapsulation is not enabled.

Command Modes

ATM VC configuration VC class configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB

Usage Guidelines

The **protocol pppovlan dot1q** command enables an ATM PVC to support PPPoE over 802.1Q VLAN traffic that uses bridged RFC 1483 encapsulation.

An ATM PVC will drop 802.1Q traffic that is configured for non-PPPoE VLANs.

PPPoE over 802.1Q VLANs over ATM is supported on the PPPoE server only.

Examples

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

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

Related Commands

Command	Description
debug pppoe	Displays debugging information for PPPoE sessions.

provision code

To specify the provision code to be used by the customer premise equipment (CPE), use the **provision code** command in TR-069 Agent configuration mode.

provision code *code-string*

Syntax Description

code-string	The provision code.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to specify the provision code to be used by the CPE:

```
Device(config-cwmp)# provision code ABCD
```

pvc-in-range

To configure an individual permanent virtual circuit (PVC) within a PVC range, use the **pvc-in-range** command in PVC range configuration mode. To delete the individual PVC configuration, use the **no** form of this command.

pvc-in-range[*pvc-name*][*vpi/vci*]

no pvc-in-range[*pvc-name*][*vpi/vci*]

Syntax Description

pvc-name	(Optional) Name given to the PVC. The PVC name can have a maximum of 15 characters.
vpi /	(Optional) ATM network virtual path identifier (VPI) for this PVC. In the absence of the "/" and a *vpi* value, the *vpi* value defaults to 0. The *vpi* value ranges from 0 to 255.
vci	(Optional) ATM network virtual channel identifier (VCI) for this PVC. The *vci* value ranges from 32 to 2047.

Command Default

No default behavior or values

Command Modes

PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **pvc-in-range** command defines an individual PVC within a PVC range and enables PVC-in-range configuration mode.

Examples

In the following example, a PVC called "pppoa" is deactivated. The PVC "pppoa" is an individual PVC within a configured PVC range.

```
pvc-in-range pppoa 0/130
 shutdown
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send**command in global configuration mode. To restore the default, use the **no**form of this command.

radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] [**3gpp2**]

no radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] [**3gpp2**]

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Due to the Internet Engineering Task Force (IETF) requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default. However, if your servers require this information, then the **cisco-nas-port** keyword can be used to return the Cisco NAS port VSA.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3gpp2) Cisco VSAs to this packet type.

Command Default

NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
Cisco IOS XE Release 3.3S.	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send**command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

In the preceding example, "protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; "attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and "sep" is "=" for mandatory attributes and "*" for optional attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco "multiple named ip address pools" feature to be activated during IP authorization (during the PPP Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a "NAS Prompt" user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, see RFC 2138, Remote Authentication Dial-In User Service (RADIUS).

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Router(config)# radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas port extended	Replaces the NAS-Port attribute with RADIUS IETF attribute 26 and displays extended field information.

range pvc

To define a range of ATM permanent virtual circuits (PVCs), use the **range pvc** command in interface configuration mode or subinterface configuration mode. To delete the range of ATM PVCs, use the **no** form of this command.

range{[*rangem-name*]} *start-vci*[*end-vpi/*]*end-vci*

no range [*range-name*] **pvc**

Syntax Description

range-name	(Optional) Name of the range. The range name can be a maximum of 15 characters.
start-vpi /	(Optional) Beginning value for a range of virtual path identifiers (VPIs). In the absence of the "/" and a *vpi* value, the *vpi* value defaults to 0. The *vpi* value ranges from 0 to 255.
start-vci /	Beginning value for a range of virtual channel identifiers (VCIs). The *vci* value ranges from 32 to 65535.
end-vpi /	(Optional) End value for a range of virtual path identifiers (VPIs). In the absence of an *end-vpi* value, the *end-vpi* value defaults to the *start-vpi* value. The *vpi* value ranges from 0 to 255.
end-vci	End value for a range of virtual channel identifiers (VCIs). The *vci* value ranges from 32 to 65535.

Command Default

An ATM PVC range is not configured.

Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

The **range pvc**command defines a range of PVCs and enables PVC range configuration mode.

The number of PVCs in a range can be calculated using the following formula:

number of PVCs = (*end-vpi* - *start-vpi* + 1) x (*end-vci* - *start-vci* +1).

The *start-vpi* argument may be omitted if it is zero. The *end-vpi* argument may be omitted, but if it is omitted, it is assigned the value of *start-vpi* . The *end-vpi* and *end-vci* arguments are always greater than or equal to *start-vpi* and *start-vci* respectively.

When applied to multipoint subinterfaces, the **range pvc** command creates a range of ATM PVCs. When applied to point-to-point subinterfaces, the **range pvc** command creates range of PVCs and a corresponding range of point-to-point subinterfaces.

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

Examples

Examples

In the following example, 100 PVCs with VCI values from 100 to 199 for each VPI value from 0 to 4 are created for a PVC range called "range-pppoa-1". This configuration creates a total of 500 PVCs in the range. PVC parameters are then configured for the range.

```
interface atm 6/0.110 multipoint
 range range-pppoa-1 pvc 100 4/199
  class-range class-pppoa-1
  ubr 1000
  encapsulation aal5snap
  protocol ppp virtual-Template 2
```

Examples

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

```
interface atm 6/0.200 point-to-point
 ip unnumbered loopback 1
 atm route-bridged ip
 range range1 pvc 1/200 1/299
  # end
```

Related Commands

Command	Description
pvc-in-range	Configures an individual PVC within a PVC range.

rbe nasip

To specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove the specification, use the **no** form of this command.

rbe nasip *interface-type number*

no rbe nasip

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

No IP address is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

The **rbe nasip** command is used to configure support for the DHCP relay agent information option (option 82) for an ATM routed bridge encapsulation (RBE).

Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the **ip dhcp relay information option** command for the **rbe nasip** command to be effective.

Examples

The following example shows how to enable support for DHCP option 82 on the DHCP relay agent by 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. ATM RBE is configured on ATM subinterface 4/0.1.

```
ip dhcp-server 10.1.1.1
!
```

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM 4/0
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.1.1.1
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
router eigrp 100
 network 10.0.0.0
!
rbe nasip loopback 0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

relay pppoe bba-group

To configure the PPP over Ethernet (PPPoE) broadband access (BBA) group that responds to PPPoE Active Discovery (PAD) messages, use the **relay pppoe bba-group** command in VPDN group or VPDN template configuration mode. To unconfigure the group, use the **no** form of this command.

relay pppoe bba-group *pppoe-bba-group-name*

no relay pppoe bba-group *pppoe-bba-group-name*

Syntax Description

pppoe-bba-group-name	Name of the PPPoE BBA group.

Command Default

No PPPoE BBA group is configured to respond to PAD messages.

Command Modes

VPDN group configuration VPDN template configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

On the router that responds to relayed PAD messages, this command configures a PPPoE group and attaches it to a virtual private dialup network (VPDN) group or VPDN template that accepts dial-in calls for Layer 2 Tunnel Protocol (L2TP). The relayed PAD messages will be passed from the VPDN L2TP tunnel or session to the PPPoE broadband group for receiving the PAD response.

Examples

The following partial example shows how to configure a tunnel switch or L2TP tunnel server to respond to PAD messages. The **relay pppoe bba-group** command configures PPPoE "group-1", which is attached to accept dial-in VPDN group "Group-A".

```
.
.
.
vpdn-group Group-A
! Configure an L2TP tunnel for PPPoE Relay
 accept-dialin
  protocol l2tp
.
.
.
 terminate-from hostname LAC-1
 relay pppoe bba-group group-1
.
.
```

```
.
! Configure the PPPoE group to respond to the relayed PAD messages
bba-group pppoe group-1
 service profile profile-1
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

request outstanding

To set the count for the number of requests that can be sent by the customer premise equipment (CPE) to the auto-configuration server (ACS) without receiving an acknowledgement, use the **request outstanding** command in TR-069 Agent configuration mode.

request outstanding *request-count*

Syntax Description

request-count	The count for the number of requests. The range for the request count is 0 to 10. The default value is 5.

Command Default

The count is set to 5.

Command Modes

TR-069 Agent configuration (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to set the count to 6 for the number of requests that can be sent by the CPE to the ACS without receiving an acknowledgement:

```
Device(config-cwmp)# request outstanding 6
```

rx-speed

To configure the required speed on the ATM virtual circuit (VC) carrying the PPPoX session, and to transfer this information into attribute-value (AV) pair 38 from the Layer 2 Tunnel Protocol (L2TP) Access Concentrator (LAC) to the L2TP network server (LNS) for asymmetric digital subscriber line (DSL) sessions, use the **rx-speed**command in PVC class, PVC-in-range, or PVC range configuration mode. To reset the variable to have the same value as that passed in AVP 24, use the **no** form of this command.

rx-speed *incoming-cell-rate*

no rx-speed

Syntax Description

incoming-cell-rate	Incoming cell rate for L2TP AVP 38, in kb/s.

Command Default

The same value as that passed in AVP 24.

Command Modes

PVC-class (config-if-atm-vc) PVC-in-range (cfg-if-atm-range-pvc) PVC range (config-if-atm-range)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

To allow L2TP to send AVP 38 with the required value from LAC to LNS for DSL services, use the **rx-speed** command in PVC, PVC-in-range, or PVC range configuration mode.

The configured speed is transported to the LNS, which validates the session within AVP 24 and AVP 38.

Examples

The following examples show how L2TP sends AVP 38 with the required value to the LNS in PVC-class, PVC range, and PVC-in-range configuration modes:

Examples

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# pvc 0/600
Router(config-if-atm-vc)# rx-speed 128
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# exit
```

Examples

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range1 pvc 100 4/199
Router(config-if-atm-range)# pvc-in-range 0/300 45/54
Router(cfg-if-atm-range-pvc)# rx-speed 200
Router(cfg-if-atm-range-pvc)# shutdown
```

Examples

```
Router(config)# interface atm 6/0.110 multipoint
Router(config-subif)# range range-pppoa-1 pvc 100 4/199
Router(config-if-atm-range)# rx-speed 400
Router(config-if-atm-range)# exit
```

Related Commands

Command	Description
encapsulation (ATM)	Configures the AAL and encapsulation type for an ATM VC, VC class, VC, bundle, or PVCs.
pvc	Creates or assigns a name to an ATM PVC, to specify the encapsulation type on an ATM PVC, and to enter ATM VC configuration mode.
pvc-in-range	Configures an individual PVC within a PVC range.
range pvc	Defines a range of ATM PVCs.

service deny

To deny service for the Subscriber Service Switch (SSS) policy, use the **service deny**command in subscriber profile configuration mode. To remove the configuration, use the **no** form of this command.

service deny

no service deny

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **service deny** command denies service to a subscriber for the SSS policy defined with the **subscriber profile**command..

Examples

The following example denies service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service deny
```

Related Commands

Command	Description
service local	Enables local termination service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
service vpdn group	Provides VPDN service for the SSS policy.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

service local

To define local termination service for the Subscriber Service Switch (SSS) policy, use the **service local**command in subscriber profile configuration mode. To remove the service, use the **no** form of this command.

service local

no service local

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **service local**command is used to configure local termination service for the SSS policy defined with the **subscriber profile**command.

Examples

The following example provides local termination service to users in the domain cisco.com:

```
!
subscriber profile cisco.com
 service local
```

Related Commands

Command	Description
service deny	Denies service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
service vpdn group	Provides VPDN service for the SSS policy.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

service name match

To force the Point to Point Protocol over Ethernet (PPPoE) server to match the service name received in the PPPoE Active Discovery Initiation (PADI) message, use the **service name match** command in BBA group configuration mode. To disable the configuration, use the **no** form of this command.

service name match

no service name match

Syntax Description

This command has no arguments or keywords.

Command Default

No services are configured.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB	This command was introduced.

Usage Guidelines

This command forces the PPPoE server to match the service-name received in the PADI message from the PPPoE client, to one of the PPPoE service names in the policy map type service list with its name configured as service profile before it responds. When a match is found, a Point Protocol over Ethernet Active Discovery Offer (PADO) message is returned to the PPPoE client in response to the PADI message received.

Examples

The following example illustrates service name match configuration:

```
Router(config)# bba-group pppoe
 name1
Router(config-bba-group)# service profile
 list1
Router(config-bba-group)# service name match
Router(config-bba-group)# policy-map type service
 list1
Router(config-bba-group)# pppoe service name
Router(config-bba-group)# pppoe service name1
The following example illustrates how the PPPoE service profile is configured. The service
 name match requires the requested service to match either service-1 or another-service:
Router(config)# bba-group pppoe
 name1
Router(config-bba-group)# service profile
 list1
Router(config-bba-group)# service name match
Router(config-bba-group)# policy-map type service
 list1
Router(config-bba-group)# pppoe service
 service-1
Router(config-bba-group)# pppoe service
 another-service
```

Related Commands

Command	Description
pppoe service	Adds a PPPoE service name to a local subscriber profile.
bba-group pppoe	Creates a PPPoE profile
policy-map type service	Creates or modifies a service policy map, which is used to define an ISG subscriber service.

service netflow timeout

To configure NetFlow PXF timers for active and inactive flow entries in the Cisco IOS NetFlow cache on the Cisco 10000 series router, use the s**ervice netflow timeout**command in global configuration mode.

service netflow timeout [**active**| **inactive**] *value*

Syntax Description

active	Specifies the NetFlow PXF timeout for active flow entries.
inactive	Specifies the NetFlow PXF timeout for inactive flow entries.
value	Specifies the NetFlow PXF timeout, in seconds. Range is from 0 to 4292967295.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB2	This command was introduced in Cisco IOS Release 12.2(28)SB2 and implemented on the Cisco 10000 series router.

Usage Guidelines

This command is not supported for customer use without Cisco Technical Assistance Center (TAC) authorization.

If you configure the timers, the router does not retain your settings on PXF or Performance Routing Engine (PRE) reloads. On PXF and PRE reloads, the active timeout reverts to 60 seconds and the inactive timeout to 15 seconds.

We recommend that the active timeout value be larger than the inactive timeout value. Also, we recommend that you do not configure the inactive timeout lower than 15 seconds to prevent the sending of excessive flow records from the PXF to the Route Processor (RP).

The service internal command is required to configure the NetFlow PXF timers.

Examples

The following example shows how to set the NetFlow PXF active timeout to 90 seconds:

```
Router> enable
Router# configure terminal
Router(config)# service internal
Router(config)# service netflow timeout active 90
Router(config)# end
```

Related Commands

Command	Description
show ip cache flow	Displays a summary of NetFlow accounting statistics.

service profile

To assign a subscriber profile to a PPP over Ethernet (PPPoE) profile, use the **service profile** command in BBA group configuration mode. To remove a subscriber profile assignment from a PPPoE profile, use the **no** form of this command.

service profile *subscriber-profile-name* [**refresh** *minutes*]

no service profile *subscriber-profile-name* [**refresh** *minutes*]

Syntax Description

subscriber-profile-name	Name of the subscriber profile to be assigned to a PPPoE profile.
refresh	(Optional) Causes the cached PPPoE configuration to be timed out and reread from the subscriber profile.
minutes	Number of minutes after which the cached PPPoE configuration will be timed out. The range is from 2 to 44640 minutes. There is no default.

Command Default

A subscriber profile is not assigned to a PPPoE profile.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

A subscriber profile contains a list of PPPoE service names. Use the **service profile** command to assign a subscriber profile to a PPPoE profile. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile.

A subscriber profile can be configured locally on the router or remotely on a AAA server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **service profile** command with the **refresh** keyword and the *minutes* argument to cause the cached PPPoE configuration to be timed out after a specified number of minutes. When the cached PPPoE configuration is timed out, the PPPoE profile rereads the configuration in the subscriber profile.

Examples

The following example shows how to assign a subscriber profile called "customer_tunnels" to a PPPoE profile called "group_A":

```
!
! Configure the AAA default authorization method
aaa new-model
aaa authorization network default group radius
!
! Configure the PPPoE profile
bba-group pppoe group_A
 virtual-template 1
 sessions per-vc  5
 service profile customer_tunnels
!
! Attach the PPPoE profile to PVCs
interface atm1/0.1
 pvc 2/200
  protocol PPPoE group pppoe_group_A
!
interface atm1/0.2
 pvc 3/300
  protocol PPPoE group pppoe_group_A
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
show pppoe derived	Displays the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

service relay

To enable relay of PPPoE Active Discovery (PAD) messages over a Layer 2 Tunnel Protocol (L2TP) tunnel, use the **service relay**command in subscriber profile configuration mode. To disable message relay, use the **no** form of this command.

service relay pppoe vpdn group *vpdn-group-name*

no service relay pppoe vpdn group *vpdn-group-name*

Syntax Description

pppoe	Provides relay service using PPP over Ethernet (PPPoE) using a virtual private dialup network (VPDN) L2TP tunnel for the relay.
vpdn group *vpdn-group-name*	Provides VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **service relay**command is configured as part of a subscriber profile. The subscriber profile name is obtained based on the authorization key specified in the **service profile**PPPoE broadband access (BBA) group configuration command. See the "Examples" section for clarification.

Examples

The following example configures the group named Sample1.net to contain outgoing tunnel information for the relay of PAD messages over an L2TP tunnel:

```
subscriber profile profile-1
! Configure profile for PPPoE Relay
 service relay pppoe vpdn group Sample1.net
!
bba-group pppoe group-1
 virtual-template 1
 service profile profile-1
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
service	Configures the type of service that will be granted to a subscriber.
service profile	Assigns a subscriber profile to a PPPoE profile.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.

sessions threshold

To configure the global threshold value of PPP over Ethernet (PPPoE) sessions on the Cisco ASR 1000 Series Aggregation Services Router, use the **sessions threshold** command in BBA group configuration mode. To disable the global threshold value, use the **no** form of this command.

sessions threshold *number*

no sessions threshold *number*

Syntax Description

number	Maximum number of permissible PPPoE sessions. Range: 1 to 65535.

Command Default

The global threshold value is not set.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to configure 1000 PPPoE sessions as the global threshold value on the **Cisco**ASR 1000 router:

```
Router# configure terminal
Router(config)# bba-group pppoe global
Router(config-bba-group)# sessions threshold 1000
```

Related Commands

Command	Description
pppoe-sessions threshold	Configures the per-physical interface threshold value of the ASR1000 router.

service vpdn group

To provide virtual private dialup network (VPDN) service for the Subscriber Service Switch policy, use the **service vpdn group** command in subscriber profile configuration mode. To remove VPDN service, use the **no** form of this command.

service vpdn group *vpdn-group-name*

no service vpdn group *vpdn-group-name*

Syntax Description

vpdn-group-name	Provides the VPDN service by obtaining the configuration from a predefined VPDN group.

Command Default

This command is disabled by default.

Command Modes

Subscriber profile configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **service vpdn group** command provides VPDN service by obtaining the configuration from a predefined VPDN group for the SSS policy defined with the **subscriber profile** command.

Examples

The following example provides VPDN service to users in the domain cisco.com and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to dialed number identification service (DNIS) 1234567 and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node) and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile host:lac
 service vpdn group 1
```

Related Commands

Command	Description
service deny	Denies service for the SSS policy.
service local	Enables local termination service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
subscriber profile	Defines the SSS policy for searches of a subscriber profile database.
vpdn-group	Associates a VPDN group to a customer or VPDN profile.

sessions max limit

To configure the PPP over Ethernet (PPPoE) global profile with the maximum number of PPPoE sessions that will be permitted on a router and to set the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated, use the **sessions max limit**command in BBA group configuration mode. To remove these settings, use the **no** form of this command.

sessions max limit *number-of-sessions* [**threshold** *number-of-sessions*]

no sessions max limit *number-of-sessions* [**threshold** *number-of-sessions*]

Syntax Description

number-of-sessions	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the total number of interfaces on the router.
threshold	(Optional) Sets the PPPoE session-count threshold at which an SNMP trap will be generated.
number-of-sessions	(Optional) Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the total number of interfaces on the router.

Command Default

There is no default number of sessions. The default threshold value is the configured number of sessions.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command can be used only in a global PPPoE profile.

The **snmp-server enable traps pppoe** command must be configured in order for SNMP traps to be generated when the PPPoE session-count threshold is reached.

Examples

The following example shows the global PPPoE profile configured with a maximum PPPoE session limit of 8000 sessions. The PPPoE session-count threshold is set at 7000 sessions, so when the number of PPPoE sessions on the router reaches 7000, an SNMP trap will be generated.

```
Router> enable
Router(config)# bba-group pppoe global

Router(config-bba-group)# virtual-template 1

Router(config-bba-group)# sessions max limit 8000 threshold 7000
Router(config-bba-group)# sessions per-vc limit 8

Router(config-bba-group)# sessions per-mac limit 2
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions permitted over a VC and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.
snmp-server enable traps pppoe	Enables PPPoE session-count SNMP notifications.

sessions per-mac iwf limit

To set the maximum number of Interworking Functionality (IWF) sessions allowed per MAC address in a PPP over Ethernet (PPPoE) profile, use the **sessions per-mac iwf limit**command in BBA group configuration mode. To remove this setting, use the **no** form of this command.

sessions per-mac iwf limit *per-mac-limit*

no sessions per-mac iwf limit *per-mac-limit*

Syntax Description

per-mac-limit	Maximum number of PPPoE sessions that can be sourced from a MAC address.

Command Default

The normal MAC address session limit (default is 100 sessions) is applied to IWF sessions.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **sessions per-mac iwf limit**command to configure a PPPoE profile with the maximum number of IWF-specific sessions allowed per MAC address.

You cannot configure PPPoE session limits in PPPoE profiles and in virtual private dialup network (VPDN) groups simultaneously. You also cannot configure session limits in PPPoE profiles and directly on PPPoE ports (Ethernet interface, VLAN, or permanent virtual circuit [PVC]) simultaneously.

Examples

The following example shows a limit of two PPPoE sessions per MAC address configured in the global PPPoE profile:

```
bba-group pppoe global
 virtual-template 1
 sessions max limit 8000 threshold-sessions 7000
 sessions per-vc limit 8
 sessions per-mac iwf limit 2
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.

sessions per-mac limit

To set the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile, use the **sessions per-mac limit**command in BBA group configuration mode. To remove this setting, use the **no** form of this command.

sessions per-mac limit *per-mac-limit*

no sessions per-mac limit

Syntax Description

per-mac-limit	Maximum number of PPPoE sessions that can be sourced from a MAC address. The default is 100 sessions.

Command Default

The default limit is 100 sessions per-MAC.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Aggregation Service Routers.

Usage Guidelines

Use the **sessions per-mac limit**command to set the maximum number of PPP over Ethernet (PPPoE) sessions allowed per MAC address in a PPPoE profile.

You cannot configure PPPoE session limits in PPPoE profiles simultaneously. You also cannot configure the PPPoE profiles directly on PPPoE ports (Ethernet interface, VLAN, or permanent virtual circuit (PVC)) simultaneously.

Examples

The following example shows a limit of two PPPoE sessions per MAC address configured in the global PPPoE profile:

```
bba-group pppoe global
 virtual-template 1
sessions per-mac limit 2
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.

sessions per-vc limit

To set the maximum number of PPP over Ethernet (PPPoE) sessions to be established over a virtual circuit (VC) in a PPPoE profile and to set the PPPoE session-count threshold at which a Simple Network Management Protocol (SNMP) trap will be generated, use the **sessions per-vc limit**command in BBA group configuration mode. To remove this specification, use the **no** form of this command.

sessions per-vc limit *per-vc-limit* [**threshold** *threshold-value*]

no sessions per-vc limit

Syntax Description

per-vc-limit	Maximum number of PPPoE sessions that can be established over an ATM PVC. The default is 100 sessions.
threshold	(Optional) Sets the PPPoE session-count threshold at which an SNMP trap is generated.
threshold-value	(Optional) Number of PPPoE sessions that causes an SNMP trap to be generated.

Command Default

The default limit is 100 sessions per-VC.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.4	This command was introduced on the Cisco ASR 1000 Series Aggregation Service Routers.

Usage Guidelines

Use the **sessions per-vc limit**command to configure a PPPoE profile with the maximum number of PPPoE sessions that will be allowed per VC.

You cannot configure session limits in PPPoE profiles and directly on permanent virtual circuits (PVCs) simultaneously.

The **snmp-server enable traps pppoe** command must be configured in order for SNMP traps to be generated when the PPPoE session-count threshold is reached.

Examples

The following example shows a limit of eight PPPoE sessions per VC configured in the PPPoE profile "vpn1":

```
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 600 threshold 400
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions per VLAN in a PPPoE profile.
snmp-server enable traps pppoe	Enables PPPoE session-count SNMP notifications.

sessions per-vlan limit

To specify the maximum number of PPP over Ethernet (PPPoE) sessions permitted per VLAN in a PPPoE profile, use the **sessions per-vlan limit**command in BBA group configuration mode. To remove this specification, use the **no** form of this command.

sessions per-vlan limit *per-vlan-limit* **inner** *inner-vlan-limit*

no sessions per-vlan limit *per-vlan-limit*

Syntax Description

per-vlan-limit	Maximum number of PPPoE sessions permitted under each VLAN, the permitted range between 1 and 65535.
inner	The inner session limit per QinQ inner Vlan-id.
inner-vlan-limit	Maximum inner sessions per QinQ inner Vlan-id, the permitted range between 1 and 65535.

Command Default

The default number of sessions per QinQ inner Vlan-id is 100.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated.
12.2(28)SB	This command was integrated.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

Use the **sessions per-vlan limit**command to configure a PPPoE profile with the maximum number of PPPoE sessions that will be allowed per VLAN.

You cannot configure session limits in PPPoE profiles and directly on VLANs simultaneously.

Examples

The following example shows a limit of 200 PPPoE sessions per VLAN configured in the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# virtual-template 1
Router(config-bba-group)# sessions per-vlan limit 200 inner 100
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
sessions max limit	Configures a PPPoE global profile with the maximum number of PPPoE sessions that will be permitted on a router and sets the PPPoE session-count threshold.
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.

sessions pre-auth limit ignore

To enable the local session limit configured on the BRAS or LAC to override the per-NAS-port session limit downloaded from the RADIUS server when Subscriber Service Switch (SSS) preauthorization is configured, use the sessions pre-auth limit ignore command in BBA group configuration mode. To disable the function, use the no form of this command.

sessions pre-auth limit ignore

no sessions pre-auth limit ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The session limit downloaded from RADIUS takes precedence over the local limit.

Command Modes

BBA group configuration mode

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	Ths command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

The sessions pre-auth limit ignore command is used to enable the PPPoE Session Limit Local Override feature. This feature is useful only when you have configured SSS preauthorization on the BRAS or LAC. If preauthorization is not enabled, the sessions pre-auth limit ignore command has no effect.

When the subscriber access pppoe pre-authorize nas-port-id command is enabled (that is, SSS preauthorization on the LAC is enabled), the PPPoE per-NAS-port session limit downloaded from the RADIUS customer profile database overrides any session limit per VC and per VLAN that you have configured locally.

When the sessions pre-auth limit ignore command is used and SSS preauthorization is configured, the LAC handles the session limit checking as if the subscriber access pppoe pre-authorize nas-port-id command were disabled; that is, the locally configured per-VC or per-VLAN session limit is applied instead of downloading the PPPoE per-NAS-port session limits that are maintained in the RADIUS server.

If you specify the sessions pre-auth limit ignore command and enable preauthorization, but there are no locally configured per-port session limits, then per-NAS-port session limits downloaded from RADIUS are applied.

Examples

The following example enables the local session limit configured on the LAC to override the per-NAS-port session limit configured on the RADIUS server for the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# sessions pre-auth limit ignore
```

The following example re-enables the standard functionality of the the subscriber access pppoe pre-authorize nas-port-id command for the PPPoE profile "vpn1":

```
Router(config)# bba-group pppoe vpn1
Router(config-bba-group)# no sessions pre-auth limit ignore
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.
subscriber access ppoe pre-authorize nas-port-id	Configures a NAS to enable SSS to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name.

sessions per-vlan throttle

To control and throttle the number of PPP over Ethernet (PPPoE) session establishment attempts per MAC address in a particular VLAN, use the **sessions per-vlan throttle** command in BBA group configuration mode. To disable this configuration, use the **no** form of this command.

sessions per-vlan throttle *number-of-sessions session-length session-delay*

no sessions per-vlan throttle *number-of-sessions session-length session-delay*

Syntax Description

number-of-sessions	Maximum number of discovery attempts per VLAN for a given MAC address.
session-length	Permitted time in seconds for the maximum number of sessions per VLAN.
session-delay	The time in seconds that further PPPoE session establishment attempts are blocked from the MAC address.

Command Default

No configuration to throttle the PPPoE sessions per VLAN.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(33)SB	This command was introduced.
Cisco IOS XE Release 2.4.0	This command was integrated. The **throttle**keyword was added.

Usage Guidelines

This command is used to throttle PPPoE discovery attempts in an aggregation deployment when multiple CPEs share the same MAC address, in different VLANs. It allows a per-VLAN throttling mechanism on a per-MAC address basis. The **sessions per-mac throttle** command works in a Broadband Aggregation System (BRAS) global scenario, since the same MAC address is seen in different VLANs.

If the value specified in the *number-of-sessions*argument, in a time-interval defined by the *session-length*argument is exceeded on a particular VLAN, then the particular MAC address is throttled for the period specified in the *session-delay*argument.

Examples

In the following example, a maximum of 100 sessions can be established on each MAC address on each VLAN, in 5 seconds, with a 5-second delay, before a new session request is allowed. The 101st session request causes a 5-second delay before a new session request is allowed:

```
Router(config)# bba-group pppoe global
Router(config-bba-group)# sessions per-vlan
 throttle 100 5 5
```

Related Commands

Command	Description
sessions per-mac throttle	Limits the number of PPPoE session requests that can be made from a single MAC address.
sessions per-vc throttle	Limits the number of PPPoE session requests that can be made from a single VC.

session retry limit

To set the session retry count. Whenever a TR-069 Agent session establishment fails with the auto-configuration server (ACS), the session will be retried for a specified number of times. Use the **session retry limit** command in TR-069 Agent configuration mode.

session retry limit *session-count*

Syntax Description

session-count	The number of retry count sessions. The range for the session count is 0 to 15. The default value is 11.

Command Default

The session retry count is set to 11.

Command Modes

TR-069 Agent configuration mode (config-cwmp)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows how to set the session retry count to 10 whenever a TR-069 Agent session establishment fails with the ACS:

```
Device(config-cwmp)# session retry limit 10
```

sessions throttle

To configure PPP over Ethernet (PPPoE) connection throttling, which limits the number of PPPoE session requests that can be made from a Virtual Circuit (VC) or a Media Access Control (MAC) address within a specified period of time, use the **sessions throttle** command in BBA group configuration mode. To remove this limit, use the **no** form of this command.

sessions {**per-mac**| **per-vc**| **per-vlan**} **throttle** *session-requests session-request-period blocking-period*

no sessions {**per-mac**| **per-vc**| **per-vlan**} **throttle** *session-requests session-request-period blocking-period*

Syntax Description

per-mac	Limits the number of PPPoE session requests that can be made from a single MAC address.
per-vc	Limits the number of PPPoE session requests that can be made from a single VC.
per-vlan	Limits the number of PPPoE session requests that can be made from a single VLAN.
session-requests	Number of PPPoE session requests that will be allowed within a specified period of time. Range is from 1 to 100000.
session-request-period	Period of time, in seconds, during which a specified number of PPPoE session requests will be allowed. Range is from 1 to 3600.
blocking-period	Period of time, in seconds, during which PPPoE session requests will be blocked. This period begins when the number of PPPoE session requests from a VC, VLAN, or MAC address exceeds the configured *session-requests* value within the configured *session-request-period*. Range is from 0 to 3600.

Command Default

The number of PPPoE session requests that can be made within a specific period of time is not limited.

Command Modes

BBA group configuration (config-bba-group)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. The **per-vlan**keyword was added.

Usage Guidelines

Continuous requests to initiate PPPoE sessions can seriously affect the performance of a router and RADIUS server. Use the **sessions throttle** command to configure the PPPoE server to limit the number of requests for PPPoE sessions that can be made from a MAC address or VC during a configured period of time.

If a client exceeds the configured number of allowable session requests (*session-requests*) within the configured time limit (*session-request-period*), the PPPoE server accepts only the allowable number of session requests and blocks the MAC address or VC from making any more requests for a configured period of time (*blocking-period*).

After the *blocking-period* expires, the PPPoE server will again accept the configured number of session requests from the MAC address or VC within the configured *session-request-period*.

Note All the Interworking Functionality (IWF) sessions may have a similar mac adddress. The **sessions per-mac iwf limit** command enables you to define how many sessions can be terminated per mac with an IWF tag set.

Note The **sessions per-mac throttle** command is applicable to both IWF and non-IWF sessions. Throttling per mac on IWF sessions can seriously affect the call setup for such sessions as each IWF session may use the same MAC address. Therefore it is not recommended to throttle the IWF sessions.

Examples

The following example shows the configuration of per-MAC, per-VC, and per-VLAN PPPoE connection throttling in PPPoE profile "grp1":

```
bba-group pppoe grp1
 virtual-template 1
 sessions per-mac throttle 10 60 300
 sessions per-vc throttle 100 30 300
 sessions per-vlan throttle 50 60 300
interface ATM2/0.1 multipoint
 pvc 2/100
  encapsulation aal5snap
  protocol pppoe group grp1
interface virtual-template1
 ip address negotiated
 no peer default ip address
 ppp authentication chap
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

Command	Description
sessions per-mac limit	Sets the maximum number of PPPoE sessions allowed per MAC address in a PPPoE profile.
sessions per-vc limit	Sets the maximum number of PPPoE sessions to be established over a VC in a PPPoE profile and sets the PPPoE session-count threshold.
sessions per-vlan limit	Sets the maximum number of PPPoE sessions to be established over a VLAN in a PPPoE profile and sets the PPPoE session-count threshold.

show access-list template through vpn service

show access-list template

To display information about access control lists (ACLs), use the **show access-list template** command in privileged EXEC mode.

show access-list template {**summary**| *aclname*| **exceed** *number*| **tree**}

Syntax Description

summary	Displays summary information about ACLs.
aclname	Displays information about the specified ACL.
exceed *number*	Limits the results to template ACLs that replace more than the specified *number* of individual ACLs.
tree	Provides an easily readable summary of the frequency of use of each of the ACL types that the template ACL function sees.

Command Modes

Privileged EXEC#

Command History

Cisco IOS Release	Description
12.2(27)SBKA	This command was introduced on the Cisco 10000 series router.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

This section provides examples of the different forms of the **show access-list template** command.

Examples

The following example shows output from the **show access-list template summary** command:

```
Router# show access-list template summary

Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

Output from this command includes:

- Maximum number of rules per template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates

Examples

The following example shows output from the **show access-list template** *aclname* command:

```
Router# show access-list template 4Temp_1073741891108
 Showing data for 4Temp_1073741891108
 4Temp_1073741891108 peer_ip used is 172.17.2.62,
 is a parent, attached acl count = 98
 currentCRC = 59DAB725
Router# show access-list template 4Temp_1342177340101
 Showing data for 4Temp_1342177340101
 4Temp_1342177340101 idb's ip peer = 172.17.2.55,
 parent is 4Temp_1073741891108, user account attached to parent = 98
 currentCRC = 59DAB725
```

Output from this display includes:

- Peer IP of the interface associated with the named template ACL
- Name of the ACL serving as the primary user of the named template ACL
- Number of ACLs matching the template of the named template ACL
- Current cyclic redundancy check 32-bit (CRC32) value

Examples

The following example shows output from the **show access-list template exceed** *number* command:

```
Router# show access-list template exceed 49
ACL name                          OrigCRC    Count      CalcCRC
4Temp_#120795960097               104FB543   50       104FB543
```

The table below describes the significant fields shown in the display.

Table 4: show access-list template exceed Field Descriptions

Field	Description
ACL Name	Name of the template ACL. Only template ACLs that contain more than the specified number (**exceed** *number*) of child ACLs are listed.
OrigCRC	Original CRC32 value
Count	Count of ACLs that match the template ACL
CalcCRC	Calculated CRC32 value

Examples

The following example shows output from the **show access-list template tree** command:

```
Router# show access-list template tree
ACL name      OrigCRC   Count  CalcCRC
4Temp_1073741891108      59DAB725   98  59DAB725
```

The table below describes the significant fields shown in the display.

Table 5: show access-list template tree Field Descriptions

Field	Description
ACL name	Name of an ACL on the Red-Black tree
OrigCRC	Original CRC32 value
Count	Number of users of the ACL
CalcCRC	Calculated CRC32 value

show atm svc ppp

To display information about each switched virtual circuit (SVC) configured for PPP over ATM, use the **show atm svc ppp** command in privileged EXEC mode.

show atm svc ppp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

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

```
Router# show atm svc ppp
ATM Int.       VCD/Name      VPI   VCI  Type   VCSt  VA  VASt
2/0.1          10             0    60   SVC     UP   1   UP
```

The table below describes the fields shown in the display.

Table 6: show atm svc ppp Field Descriptions

Field	Description
ATM Int.	Interface on which the SVC is configured.
VCD/Name	Virtual circuit descriptor (VCD) or name associated with the SVC.
VPI	Virtual path identifier.
VCI	Virtual channel identifier.
Type	Type of virtual circuit.
VCSt	Virtual circuit state.
VA	Virtual access interface number.
VASt	Virtual access interface state.

show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics**command in user EXEC or privileged EXEC mode.

show call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

The table below describes the significant fields shown in the display.

Table 7: show call admission statistics Field Descriptions

Field	Description
Total call admission charges	Percentage of system resources being charged to the system. If you configured a resource limit, SA requests are dropped when this field is equal to that limit.
limit	Maximum allowed number of total call admission charges. Valid values are 0 to 100000.
Total calls rejected	Number of SA requests that were not accepted.
accepted	Number of SA requests that were accepted.

Field	Description
unscaled	Not related to IKE. This value always is 0.

Related Commands

Command	Description
call admission limit	Instructs IKE to drop calls when a specified percentage of system resources are being consumed.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.

show ccm clients

To display information about cluster control manager (CCM) clients on high availability (HA) dual Route Processor systems, use the **show ccm clients** command in privileged EXEC mode.

show ccm clients[**id** *ccm-group-id*]

Syntax Description

id *ccm-group-id*	(Optional) Displays information about the specified CCM group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.5S	This command was modified. The output was enhanced to include information about periodic session updates.

Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a dual Route Processor HA system. Use the **show ccm clients** command to display information about CCM clients.

Examples

The following is sample output from the **show ccm clients** command on a Cisco ASR 1000 Series Router's active processor:

```
Router# show ccm clients

CCM bundles sent since peer up:
                                        Sent            Queued for flow control
    Sync Session                        3               0
    Update Session                      1               0
    Active Bulk Sync End                1               0
    Session Down                        3               0
    ISSU client msgs                    178             0
    Dynamic Session Sync                0               0
    Periodic Update Session             3               0
    Unknown msgs                        0               0
Client events sent since peer up:
    PPP                                 15              3
    PPPoE                               8               3
    PPPoA                               0               0
    VPDN FSP                            0               0
    AAA                                 15              3
    PPP SIP                             2               0
    LTERM                               3               0
    AC                                  0               0
    VPDN LNS                            0               0
    ATOM SUB                            0               0
    Ether-Infra CCM                     0               0
```

The following is sample output from the **show ccm clients** command on a router’s active processor:

```
Router# show ccm clients

CCM bundles sent since peer up:
                                        Sent            Queued for flow control
    Sync Session                        10              1
    Update Session                      6               1
    Active Bulk Sync End                1               0
    Session Down                        10              0
    ISSU client msgs                    115             0
    Dynamic Session Sync                0               0
    Unknown msgs                        0               0
Client events sent since peer up:
    PPP                                 66
    PPPoE                               0
    PPPoA                               0
    AAA                                 44
    PPP SIP                             11
    LTERM                               11
    AC                                  0
    SSS FM                              0
    IP SIP                              0
    IP IF                               0
    DPM                                 0
    COA                                 0
```

The following is sample output from the **show ccm clients** command on a router’s standby processor:

```
Router# show ccm clients

CCM bundles rcvd since last boot:
    Sync Session                8
    Update Session              0
    Active Bulk Sync            1
    Session Down                8
    ISSU client msgs            59
    Dynamic Session Sync        0
    Unknown msgs                0
Client events extracted since last boot:
    PPP                         72
    PPPoE                       50
    PPPoA                       0
    AAA                         32
    PPP SIP                     0
    LTERM                       8
    AC                          0
    SSS FM                      0
    IP SIP                      0
    IP IF                       0
    DPM                         0
    COA                         0
    Auto Svc                    0
```

The table below describes the significant fields shown in the display. Any data not described in the table below is used for Cisco internal debugging purposes.

Table 8: show ccm clients Field Descriptions

Field	Description
Sent	Number of CCM bundles sent by the active processor since initiation on the standby processor.

Field	Description
Queued for flow control	Number of the following types of CCM bundles queued on the active processor when flow control is OFF since initiation on the standby processor: • Sync Session—Synchronization session bundles. • Update Session—Individual client update to session bundles. • Active Bulk Sync—Active processor bulk synchronization bundles. • Session Down—Session down bundles. • ISSU client msgs—In service software upgrade (ISSU) bundles. • Dynamic Session Sync—Dynamic cluster update to session bundles. • Unknown msgs—Unknown message bundles. The queued bundles will be sent when flow control is ON again.
Periodic Update Session	Cumulative number of periodic updates sent on active processor, or received on standby processor.
Client events sent since peer up	Number of client events sent since initiation on the standby processor.
CCM bundles rcvd since last boot	Number of the following types of CCM bundles received by the standby processor since initiation: • Sync Session—Synchronization session bundles. • Update Session—Individual client update to session bundles. • Active Bulk Sync—Active processor bulk synchronization bundles. • Session Down—Session down bundles. • ISSU client msgs—ISSU bundles. • Dynamic Session Sync—Dynamic cluster update to session bundles. • Unknown msgs—Unknown message bundles.

Field	Description
Client events extracted since last boot	Number of client events extracted since initiation on the standby processor.

Related Commands

Command	Description
show ccm queues	Displays CCM queue statistics.
show ccm sessions	Displays CCM session information.

show ccm queues

To display cluster control manager (CCM) queue statistics for high availability (HA) dual Route Processor systems, use the **show ccm queues** command in privileged EXEC mode.

show ccm queues

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.5S	This command was modified. The output was enhanced to include information about periodic session updates.

Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a redundant processor HA system. Use the **show ccm queues** command to display queue statistics for CCM sessions on active and standby processors. This command is generally used only by Cisco engineers for internal debugging of CCM processes.

Examples

The following is sample output from the **show ccm queues** command on a Cisco ASR 1000 Series Router. No field descriptions are provided because command output is used for Cisco internal debugging purposes only.

```
Router# show ccm queues

10 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 3 CCM              0    20        196        197        1          0        20
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  3 Sync Session              3        0        2        0       333      1000
 2  3 Sync Client               0        0        0        0         0         0
 3  3 Update                    2        0        1        0         0         0
 4  3 Session Down              3        0        2        0       333      1000
 5  3 Bulk Sync Begi            1        0        1        0         0         0
 6  3 Bulk Sync Cont            2        0        2        0         0         0
 7  3 Bulk Sync End             1        0        1        0         0         0
 8  3 Rcv Bulk End              0        0        0        0         0         0
 9  3 Dynamic Sync C            2        0        1        0         0         0
10  3 Going Active              0        0        0        0         0         0
11  3 Going Standby             0        0        0        0         0         0
12  3 Standby Presen            1        0        1        0         0         0
13  3 Standby Gone              0        0        0        0         0         0
```

```
15  3 CP Message              335        0       20        0         8      1000
16  3 Recr Session              0        0        0        0         0         0
17  3 Recr Update               0        0        0        0         0         0
18  3 Recr Sess Down            0        0        0        0         0         0
19  3 ISSU Session N            1        0        1        0         0         0
20  3 ISSU Peer Comm            0        0        0        0         0         0
21  3 Free Session            101        0        2        0         0         0
22  3 Sync Dyn Sessi            0        0        0        0         0         0
23  3 Recr Dyn Sessi            0        0        0        0         0         0
24  3 Session Ready             0        0        0        0         0         0
25  3 Pending Update            0        0        0        0         0         0
26  3 Cleanup All Se            0        0        0        0         0         0
27  3 Periodic Update           3        0        2        0       333      1000
28  3 Recreate Periodic Update  0        0        0        0         0         0
29  3 Enable Periodic Update    1        0        0        0         0         0
30  3 Disable Periodic Update   0        0        0        0         0         0
31  3 Modify Periodic Update    0        0        0        0         0         0

FSM Event Names           Events
 0    Invalid                   0
 1    All Ready                 3
 2    Required Not Re           1
 3    Update                    2
 4    Down                    101
 5    Error                     0
 6    Ready                     0
 7    Not Syncable              0
 8    Recreate Down             0
 9    Periodic Update           3
```

The following is sample output from the **show ccm queues** command. No field descriptions are provided because command output is used for Cisco internal debugging purposes only.

```
Router# show ccm queues

8 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 4 CCM              0     7      16167      16168        1          0         20
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1  4 Sync Session              0        0        0        0         0         0
 2  4 Sync Client               0        0        0        0         0         0
 3  4 Update                    0        0        0        0         0         0
 4  4 Session Down              0        0        0        0         0         0
 5  4 Bulk Sync Begi            1        0        1        0         0         0
 6  4 Bulk Sync Cont            2        0        2        0         0         0
 7  4 Bulk Sync End             1        0        1        0         0         0
 8  4 Rcv Bulk End              0        0        0        0         0         0
 9  4 Dynamic Sync C            0        0        0        0         0         0
10  4 Going Active              0        0        0        0         0         0
11  4 Going Standby             0        0        0        0         0         0
12  4 Standby Presen            1        0        1        0         0         0
13  4 Standby Gone              0        0        0        0         0         0
15  4 CP Message              188        0        7        0         0         0
16  4 Recr Session              0        0        0        0         0         0
17  4 Recr Update               0        0        0        0         0         0
18  4 Recr Sess Down            0        0        0        0         0         0
19  4 ISSU Session N            1        0        1        0         0         0
20  4 ISSU Peer Comm            0        0        0        0         0         0
21  4 Free Session          16103        0        1        0         0         0
22  4 Sync Dyn Sessi            0        0        0        0         0         0
23  4 Recr Dyn Sessi            0        0        0        0         0         0
24  4 Session Ready             0        0        0        0         0         0
FSM Event Names           Events
 0    Invalid                   0
 1    All Ready                 0
 2    Required Not Re           0
 3    Update                    0
 4    Down                  16103
 5    Error                     0
 6    Ready                     0
```

```
7    Not Syncable              0
8    Recreate Down             0
```

Related Commands

Command	Description
show ccm clients	Displays CCM client information.
show ccm sessions	Displays CCM session information.

show ccm sessions

To display information about cluster control manager (CCM) sessions on high availability (HA) dual Route Processor systems, use the **show ccm sessions** command in privileged EXEC mode.

show ccm sessions[**id** *ccm-group-id*]

Syntax Description

id *ccm-group-id*	(Optional) Displays information about the specified CCM group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.5S	This command was modified. The output was enhanced to include information about periodic session updates.

Usage Guidelines

The CCM manages the capability to synchronize session initiation on the standby processor of a redundant processor HA system. Use the **show ccm sessions** command to display information on CCM sessions on active and standby processors, and also to display information on subscriber redundancy policies configured using the **subscriber redundancy** command.

Examples

The following is sample output from the **show ccm sessions** command on a Cisco ASR 1000 Series Router active processor. To display information about periodic session updates, the **subscriber redundancy dynamic periodic-update interval** command must be configured.

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0x9EFFE

                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready    0           1           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    3           0           0

Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         2           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:01 -         8           -         -
         RGF Bulk Tim 00:05:00 -         0           -         -

Periodic Update:
    Number of sessions Interested in Periodic Update:  1
    Configured Periodic Update Interval(In Minutes):   10
```

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router active processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0x0
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0
Number of sessions in state Not Ready:0
Number of sessions in state Ready:       0
Number of sessions in state Dyn Sync:    0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         2           -         -
         Dynamic CPU  00:00:10 -         0           90        0
```

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router standby processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Standby - Collecting
Global ISSU state:                       Compatible, Clients Cap 0xFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   0           0           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router active processor:

```
Router# show ccm sessions

Global CCM state:                        CCM HA Active - Dynamic Sync
Global ISSU state:                       Compatible, Clients Cap 0xFFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   7424        0           0
Number of sessions in state Ready:       0           0           0
Number of sessions in state Dyn Sync:    20002       28001       0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         924         -         -
         Dynamic CPU  00:00:10 -         0           90        2
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         18          -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router standby processor:

```
Router# show ccm sessions
```

```
Global CCM state:                        CCM HA Standby - Collecting
Global ISSU state:                       Compatible, Clients Cap 0xFFE
                                         Current     Bulk Sent   Bulk Rcvd
                                         ----------- ----------- -----------
Number of sessions in state Down:        0           0           0
Number of sessions in state Not Ready:   8038        0           0
Number of sessions in state Ready:       20002       0           28001
Number of sessions in state Dyn Sync:    0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         1           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The table below describes the significant fields shown in the output, in the order in which they display. Any data not described in the table is used for Cisco internal debugging.

Table 9: show ccm sessions Field Descriptions

Field	Description
Global CCM state	Displays the processor's active or standby status and its CCM state. For example: • CCM HA Active—Dynamic Sync means that this is the active processor, standby is in STANDBY_HOT state, and CCM is ready to synchronize sessions. • CCM HA Active—Collecting means that this is the active processor and there is no standby processor. CCM can collect sessions but cannot synchronize them to a standby processor. • CCM HA Active—Bulk Sync means that this is the active processor and a standby processor is booting up. CCM is doing a bulk synchronization of sessions. • CCM HA Standby—Collecting means that this is the standby processor and is in STANDBY_HOT state. CCM is collecting sessions for synchronizing if a switchover happens.
Global ISSU state	Compatible, Clients Cap 0xFFFE0 indicates that CCM is compatible for in-service software upgrade (ISSU) clients--that is, ISSU-compatible Cisco IOS versions are running on both processors. It also means that CCM has the client capability for the clients in the bitmask 0xFFFE.
Current	CCM sessions currently ready for synchronization.
Bulk Sent	CCM sessions sent during bulk synchronization.

Field	Description
Bulk Rcvd	CCM sessions received during bulk synchronization.
Number of sessions in state Down	Sessions in the down state.
Number of sessions in state Not Ready	Sessions in the not ready state.
Number of sessions in state Ready	Sessions in the ready state.
Number of sessions in state Dyn Sync	Sessions in the dynamic synchronization state.
Timeout	Displays statistics for the following timers: • Rate—Monitors the number of sessions to be synchronized per configured time period. • Dynamic CPU—Monitors CPU limit, number of sessions, delay, and allowed calls configured for dynamic synchronization parameters. • Bulk Time Li—Monitors the time limit configured for bulk synchronization. • RF Notif Ext—Monitors redundancy facility (RF) active and standby state progressions and events. Use the subscriber redundancy command to modify parameters that these timers monitor.
Delay	Timer delay (in hh:mm:ss) for bulk and dynamic synchronization for subscriber sessions.
Remaining	Indicates remaining time in seconds before the timer expires.
Starts	Indicates the number of times the timer started.
CPU Limit	CPU usage percentage, a configurable value; default is 90 percent.
CPU Last	Indicates the last time that the CPU limit timer was running.
Number of sessions Interested in Periodic Update	Number of sessions that have registered their interest in using the periodic update feature.
Configured Periodic Update Interval (In Minutes)	Periodic update interval, in minutes, that was configured with the **subscriber redundancy dynamic periodic-update interval** command.

Related Commands

Command	Description
show ccm clients	Displays CCM client information.
show ccm queues	Displays CCM queue information.
subscriber redundancy	Configures subscriber session redundancy policies.

show checkpoint

To display a list of checkpoint clients, entitities, or statistics, use the **show checkpoint**command in privileged EXEC mode.

show checkpoint {**clients**| **entities**| **statistics**}

Syntax Description

clients	Displays detailed information about checkpoint clients.
entities	(Optional) Displays detailed information about checkpoint entities.
statistics	(Optional) Displays detailed information about checkpoint statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.(0)1S	This command was modified. The output of this command was modified to include the Buffers Held Peak statistic.

Examples

The following is sample output from the **show checkpoint clients** command:

```
Router# show checkpoint clients
                         Check Point List of Clients
 CHKPT on ACTIVE server.
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Network RF Client           3          5        On
  Total API Messages Sent:                      26
  Total Transport Messages Sent:                --
  Length of Sent Messages:                   13480
  Total Blocked Messages Sent:                  26
  Length of Sent Blocked Messages:           13480
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Messages Received:                      14
  Total Rcv Message Len:                       360
  Total Bytes Allocated:                     73800
  Buffers Held:                                  0
  Buffers Held Peak:                             3
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
############ Checked that logs were clean
No tracebacks or errmsgs in log.
######## No IPC Buffer Leaks
```

The table below describes the significant fields shown in the display.

Table 10: show checkpoint clients Field Descriptions

Field	Description
Client ID	The identification number number assigned to the client.
Entity ID	The identification number used by In-Service Software Upgrade (ISSU) for each entity within this client.
Buffers Held Peak	Displays the highest number of buffers held for a client.
Transport Frag Count	Reports the number of fragmentation buffers used.
Transport Frag Peak	Reports the high water mark of fragmentation buffers requested.

The following is sample output from the **show checkpoint statistics** command:

```
Router# show checkpoint statistics

Check Point Status
 CHKPT on ACTIVE server.
Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:            17896
TP MAX Message Size:               17992
CHKPT Pending Msg Timer:             100 ms
  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:          3781
  Total Messages Sent:              2771
  Total Sent Message Len:         382032
  Total Bytes Allocated:         2399648
  Rcv  Msg Q Peak:                    67
  Hold Msg Q Peak:                     0
  Buffers Held Peak:                 118
  Current Buffers Held:                0
  Huge Buffers Requested:              0
```

The following is sample output from the **show checkpoint entities**command:

```
Router# show checkpoint entities

Check Point List of Entities
```

```
 CHKPT on ACTIVE server.
--------------------------------------------------------------------------------
Entity ID         Entity Name
--------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            13
  Member(s) of entity 0 are:
    Client ID          Client Name
------------------------------------------
          168          DHCP Snooping
           41          Spanning-tree
          167          IGMP Snooping
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           36          LAN-Switch PAgP/LACP
           35          LAN-Switch Port Mana
           38          LAN-Switch Port Secu
          158          Inline Power Checkpo
          156          Cat4k Chassis
          172          Cat4K EbmHostMan
          157          Cat4K Link State
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show controllers shdsl

To display the status of the controller configured for single-pair high-bit-rate digital subscriber line (SHDSL) mode, use the **show controllers shdsl**command in privileged EXEC mode.

Cisco HWIC-4SHDSL and HWIC-2SHDSL

show controllers shdsl *slot number/ subslot number/*{**brief**| **detailed**}

Cisco IAD2420

show controller shdsl number

Syntax Description

brief	Provides a summary of the controller's status.
detailed	Provides a detailed report of the controller's status.
number	SHDSL controller number. The valid controller number for SHDSL mode is 0.
slot number	Identifies the slot on the router in which the HWIC is installed.
subslot number	Identifies the subslot on the router in which the HWIC is installed.
port number	Identifies the port on the router in which the HWIC is installed. By default, the Cisco HWIC-4SHDSL and HWIC-2SHDSL use port number 0.

Command Default

Controller number

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was updated for the Cisco HWIC-4SHDSL and HWIC-2SHDSL running on the Cisco 1841 router and on the Cisco 2800 and 3800 series access routers.
12.2(8)T	This command was introduced on Cisco IAD2420 series.

Usage Guidelines

This command is used to display the controller mode, the controller number, and associated statistics.

Examples

Examples

The following example displays the status of a Cisco HWIC-4SHDSL controller in slot 0, subslot 2, port 0 on a Cisco access router:

```
Router# show controllers shdsl 0/2/0 brief
Controller SHDSL 0/2/0 is UP
  Hardware is HWIC-4SHDSL, rev 2 on slot 0, hwic slot 2
  Capabilities: IMA, M-pair, 2/4 wire, Annex A, B, F & G, CPE termination
  cdb=0x43EB384C, plugin=0x43DE9410, ds=0x43E9A1C4 base=0xB8000000
  FPGA Version is REL.3.4.0, NIOSII FW:Ver 2.6, status Running
  SDC-16i HW:Rev 1.2, status UP, FW:Ver 1.2-1.1.3__57, status Running
  SDFE-4 HW:Rev 1.2, status UP, FW:Ver 1.1-1.5.2__001  , status Running
  NIOSII Firmware image: System
  SDC16i Firmware image: System
  SDFE4  Firmware image: System
  Number of pairs 4, number of groups configured 1
  Ignored CLI cmds(0), Event buffer: in use(0), failed(0)
  Group (0) is Not configured.
  Group (1) info:
        Type: M-pair over g.shdsl, status: Configure Firmware
        Interface: ATM0/2/1, hwidb: 0x43F04EA0, UTOPIA phy 1
        Configured/active num links: 2/0, bit map: 0x3/0x0
        Line termination: CPE, line mode: M-pair, Annex-B, PMMS disabled
        Line coding: 16-TCPAM, configured/actual rate: 4608/0 kbps
        SHDSL wire-pair (0) is in DSL DOWN state
        SHDSL wire-pair (1) is in DSL config state
Router#
```

Examples

The following example displays the status of the controller that is configured for SHDSL mode on a Cisco IAD2420 series IAD:

```
Router# show controller shdsl
 0
 SHDSL 0 controller UP
 SLOT 3: Globespan xDSL controller chipset
 Frame mode: Serial ATM
 Configured Line rate: 1160Kbps
 Line Re-activated 0 times after system bootup
 LOSW Defect alarm: None
 CRC per second alarm: None
 Line termination: CPE
 FPGA Revision: 9
```

Related Commands

Command	Description
controller shdsl 0	Configures the controller status and the controller number.

show cwmp map

To display the Cisco WAN Management Protocol (CWMP) map information, use the **show cwmp map** command in privileged EXEC mode.

show cwmp map {**hosttable| landevice| lanethernetinterface| routetable| wanconnectiondevice| wandevice**}

Syntax Description

hosttable	Displays host table information.
landevice	Displays LAN device profile information.
lanethernetinterface	Displays LAN Ethernet interface profile information.
routetable	Displays map forwarding table information.
wanconnectiondevice	Displays WAN connection device profile information.
wandevice	Displays WAN device profile information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show cwmp map hosttable** command, which shows the object parameter values:

```
Device# show cwmp map hosttable
Host ID IP Address      Source  MAC Address          LeaseTimeRemaining  HostName
1       172.17.0.2       DHCP   0063.6973.636f.2d61. 86255               iou132
                                6162.622e.6363.3030.
                                2e38.3430.312d.4574.
                                312f.30
```

The following is sample output from the **show cwmp map landevice** command, which shows the mapping between the interfaces available in the customer premises equipment (CPE) and the instance number of the object InternetGatewayDevice.LANDevice:

Note All the L3 Ethernet interfaces that are not configured with the **cwmp wan default** command and the logical interface (VLAN) of the switch port in the CPE are considered as a landevice.

```
Device# show cwmp map landevice
```

```
CWMP LAN Id     Interface
2               Ethernet0/1
3               Ethernet0/2
4               Ethernet0/3
5               Ethernet1/0
6               Ethernet1/1
7               Ethernet1/2
8               Ethernet1/3
```

The following is example output from the **show cwmp map lanethernetinterface** command, which shows the mapping between the instance of the object, InternetGatewayDevice.LANDevice. and InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig. This display shows all the Layer 2 switch ports grouped under a Layer 3 interface (a VLAN interface).

```
Device# show cwmp map lanethernetinterface

CWMP LAN Id     CWMP LAN Ether Id       Interface
```

The following is example output from the **show cwmp map routetable** command, which shows the static IP routes configured in the CPE. This display provides the values of the parameters of the object, InternetGatewayDevice.Layer3Forwarding.Forwarding.

```
Device# show cwmp map routetable
CWMP Id Enable  Dest Address    Dest Mask       Gateway Address Met     Interface
1       TRUE    0.0.0.0         0.0.0.0         172.16.0.2      1
```

The following is example output from the **show cwmp map wandevice** command, which shows the mapping between the interface in CPE and the instance number of the interface specified in the TR-069 Agent. This is equivalent to the CWMP object instances, InternetGatewayDevice.WANDevice.

Note By default, the ATM interface is considered a wandevice even when the **wmp wan** command is not configured. L3 Ethernet interfaces are considered as wandevice only when the **cwmp wan default**command is configured.

```
Device# show cwmp map wandevice
CWMP WAN Id     Interface
1               Ethernet0/0
```

The following is example output from the **show cwmp map wanconnectiondevice** command, which shows the instance numbers of the object InternetGatewayDevice.WANDevice.i. and InternetGatewayDevice.WANDevice.i.WANConnectionDevice.j. This command also shows the associated interface in the CPE and connection type used. The connection type value is one of the following:

- IPoE--If TR-069 Agent communicates with ACS via Ethernet Interface
- IPoA--IPoA configuration
- PPPoA--PPPoA configuration
- PPPoE--PPPoE configuration
- CIP--CIP configuration
- EoA--EoA configuration

This command also shows the VPI and VCI values of the ATM interface represented by the object, InternetGatewayDevice.WANDevice.i.WANConnectionDevice.j.

```
Device# show cwmp map wanconnectiondevice

CWMP WAN Id     CWMP WAN Conn Id        Interface               VPI     VCI     Type
1               1                       Ethernet0/0                             IPoE
```

show cwmp methods

To display the TR-069 Agent supported remote procedure call (RPC) methods and vendor profile methods, use the **show cwmp methods** command in privileged EXEC mode.

show cwmp methods

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show cwmp methods** command:

```
Device# show cwmp methods
CWMP RPC Methods Supported:
GetRPCMethods
SetParameterValues
GetParameterValues
GetParameterNames
SetParameterAttributes
GetParameterAttributes
AddObject
DeleteObject
Reboot
Download
Upload
X_00000C_SetConfiguration
X_00000C_ShowStatus
```

show cwmp parameter

To display the TR-069 Agent (also called the Cisco WAN Management Protocol [CWMP]) parameter information, use the **show cwmp parameter** command in privileged EXEC mode.

show cwmp parameter {*parameter-name*| **all**| **notify** {**active**| **all**| **forceactive**| **passive**}}

Syntax Description

parameter-name	A CWMP (TR-069 Agent) parameter.
all	Displays all CWMP (TR-069 Agent) parameters.
notify	Displays a CWMP parameter notification attribute.
active	Displays the CWMP parameters with an active notification attribute.
all	Displays all of the CWMP parameters with a notification attribute.
forceactive	Displays all of the forceactive CWMP parameters.
passive	Displays all of the CWMP parameters with a passive notification attribute.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show cwmp parameter** *parameter-name* command, which displays the value for the specified parameter:

```
Device# show cwmp parameter InternetGatewayDevice.ManagementServer.URL

Parameter = InternetGatewayDevice.ManagementServer.URL
Value = http://iou131.cisco.com/cwmp-1-0/testacs
```

The following is sample output from the **show cwmp parameter all**command, which displays all of the parameter names supported by the TR-069 Agent:

```
Device# show cwmp parameter all
InternetGatewayDevice
LANDeviceNumberOfEntries
WANDeviceNumberOfEntries
```

```
WANDevice
WANConnectionNumberOfEntries
WANCommonInterfaceConfig
WANAccessType
Layer1UpstreamMaxBitRate
Layer1DownstreamMaxBitRate
PhysicalLinkStatus
TotalBytesSent
TotalBytesReceived
TotalPacketsSent
TotalPacketsReceived
WANConnectionDevice
WANIPConnectionNumberOfEntries
WANPPPConnectionNumberOfEntries
WANIPConnection
Enable
ConnectionStatus
PossibleConnectionTypes
ConnectionType
Name
Uptime
LastConnectionError
AddressingType
ExternalIPAddress
SubnetMask
DefaultGateway
DNSEnabled
DNSServers
MACAddress
ConnectionTrigger
WANPPPConnection
Enable
ConnectionStatus
Name
Uptime
LastConnectionError
Username
Password
ExternalIPAddress
X_00000C_SubnetMask
DNSEnabled
DNSServers
MACAddress
TransportType
PPPoEACName
PPPoEServiceName
WANDSLLinkConfig
Enable
LinkStatus
LinkType
AutoConfig
DestinationAddress
ATMTransmittedBlocks
ATMReceivedBlocks
AAL5CRCErrors
ATMCRCErrors
WANEthernetInterfaceConfig
Enable
Status
MACAddress
MaxBitRate
DuplexMode
Stats
BytesSent
BytesReceived
PacketsSent
PacketsReceived
WANDSLInterfaceConfig
Enable
Status
UpstreamCurrRate
DownstreamCurrRate
UpstreamMaxRate
```

```
DownstreamMaxRate
UpstreamNoiseMargin
DownstreamNoiseMargin
UpstreamAttenuation
DownstreamAttenuation
UpstreamPower
DownstreamPower
ATURVendor
ATURCountry
ATUCVendor
ATUCCountry
TotalStart
ShowtimeStart
Stats
Total
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
Showtime
CellDelin
LinkRetrain
InitErrors
InitTimeouts
LossOfFraming
ErroredSecs
SeverelyErroredSecs
FECErrors
ATUCFECErrors
HECErrors
ATUCHECErrors
CRCErrors
ATUCCRCErrors
WANDSLConnectionManagement
ConnectionServiceNumberOfEntries
ConnectionService
WANConnectionDevice
WANConnectionService
DestinationAddress
LinkType
Name
LANDevice
LANEthernetInterfaceNumberOfEntries
LANUSBInterfaceNumberOfEntries
LANWLANConfigurationNumberOfEntries
LANHostConfigManagement
DHCPServerConfigurable
DHCPServerEnable
DHCPRelay
MinAddress
MaxAddress
ReservedAddresses
SubnetMask
DNSServers
DomainName
IPRouters
IPInterfaceNumberOfEntries
IPInterface
Enable
IPInterfaceIPAddress
IPInterfaceSubnetMask
IPInterfaceAddressingType
Hosts
HostNumberOfEntries
```

```
Host
IPAddress
AddressSource
LeaseTimeRemaining
MACAddress
HostName
LANEthernetInterfaceConfig
Enable
Status
MACAddress
MaxBitRate
DuplexMode
Stats
BytesSent
BytesReceived
PacketsSent
PacketsReceived
DeviceInfo
Manufacturer
ManufacturerOUI
ModelName
Description
SerialNumber
HardwareVersion
SoftwareVersion
SpecVersion
ProvisioningCode
UpTime
DeviceLog
ManagementServer
URL
Username
Password
PeriodicInformEnable
PeriodicInformInterval
PeriodicInformTime
ParameterKey
ConnectionRequestURL
ConnectionRequestUsername
ConnectionRequestPassword
UpgradesManaged
LANConfigSecurity
ConfigPassword
Layer3Forwarding
DefaultConnectionService
ForwardNumberOfEntries
Forwarding
Enable
Status
DestIPAddress
DestSubnetMask
SourceIPAddress
SourceSubnetMask
GatewayIPAddress
Interface
ForwardingMetric
IPPingDiagnostics
DiagnosticsState
Interface
Host
NumberOfRepetitions
Timeout
DataBlockSize
SuccessCount
FailureCount
AverageResponseTime
MinimumResponseTime
MaximumResponseTime
Time
NTPServer1
NTPServer2
NTPServer3
NTPServer4
```

```
NTPServer5
CurrentLocalTime
LocalTimeZone
LocalTimeZoneName
DaylightSavingsUsed
DaylightSavingsStart
DaylightSavingsEnd
TraceRouteDiagnostics
DiagnosticsState
Host
Timeout
MaxHopCount
ResponseTime
NumberOfRouteHops
RouteHops
HopHost
```

The following is sample output from the **show cwmp parameter notify active**command, which displays all of the parameters in which the notification attribute is set to active:

```
Device# show cwmp parameter notify active

Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceSubnetMask
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceAddressingType
```

The following is sample output from the **show cwmp parameter notify all**command, which displays all of the parameters in which the notification attribute is set:

```
Device# show cwmp parameter notify all
Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceIPAddress
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceSubnetMask
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.IPInterfaceAddressingType
Passive Notification:
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.Enable
```

The following is sample output from the **show cwmp parameter notify forceactive**command, which displays all of the forceactive parameters in the TR-069 Agent:

```
Device# show cwmp parameter notify forceactive

Forced Active Notification:
InternetGatewayDevice.DeviceInfo.SoftwareVersion
InternetGatewayDevice.DeviceInfo.ProvisioningCode
InternetGatewayDevice.ManagementServer.ConnectionRequestURL
InternetGatewayDevice.WANDevice.1.WANConnectionDevice.1.WANIPConnection.1.ExternalIPAddress
```

The following is sample output from the **show cwmp parameter notify passive**command, which displays all of the parameters in which the notification attribute is set to passive:

```
Device# show cwmp parameter notify passive

Passive Notification:
InternetGatewayDevice.LANDevice.5.LANHostConfigManagement.IPInterface.1.Enable
```

show cwmp persistent

To display all of the persistent Cisco WAN Management Protocol (CWMP) parameters stored in the NVRAM by the TR-069 Agent, use the **show cwmp persistent** command in privileged EXEC mode.

show cwmp persistent data

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show cwmp persistent data**command:

```
Device# show cwmp persistent data
InternetGatewayDevice.ManagementServer.URL
 InternetGatewayDevice.ManagementServer.Username
 InternetGatewayDevice.ManagementServer.Password
 InternetGatewayDevice.ManagementServer.PeriodicInformEnable
 InternetGatewayDevice.ManagementServer.PeriodicInformInterval
 InternetGatewayDevice.ManagementServer.PeriodicInformTime
 InternetGatewayDevice.ManagementServer.ParameterKey
 InternetGatewayDevice.ManagementServer.ConnectionRequestURL
 InternetGatewayDevice.ManagementServer.ConnectionRequestUsername
 InternetGatewayDevice.ManagementServer.ConnectionRequestPassword
 InternetGatewayDevice.ManagementServer.UpgradesManaged
```

show cwmp session

To display the TR-069 Agent session information, use the **show cwmp session** command in privileged EXEC mode.

show cwmp session

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the **show cwmp session** command when a successful session is established between the TR-069 Agent and the auto-configuration server (ACS):

```
Device# show cwmp session

CWMP Agent status: Enabled
No CWMP Session currently running
Management Server: http://iou131.cisco.com/cwmp-1-0/testacs
Connection Request URL: http://172.16.0.1/00000C/388280450/cwmp
Last successful connection request at time: 10:46:47 PST Tue Jun 17 2008
Last successful session at time: 10:46:48 PST Tue Jun 17 2008
Last failed session at time: 10:42:48 PST Tue Jun 17 2008
```

The following is sample output from the **show show cwmp session** command when a session is unable to connect between the TR-069 Agent and the ACS:

```
Device# show cwmp session

CWMP Agent status: Enabled
CWMP Session currently running
Management Server for this session: http://iou131.cisco.com/cwmp-1-0/testacs
Hold Requests for this session: 0
Max-Envelopes from ACS for this session: 1
Number of outstanding requests: 1
Requests outstanding over the session:
Inform
Inform
Requests to be sent over the session: 0
Management Server: http://iou131.cisco.com/cwmp-1-0/testacs
Connection Request URL: http://172.16.0.1/00000C/388280450/cwmp
Last successful connection request at time:
Last successful session at time: 10:39:05 PST Tue Jun 17 2008
Last failed session at time: 10:42:03 PST Tue Jun 17 2008
Session retry count: 1
```

show dsl interface atm

To display information specific to the asymmetric digital subscriber line (ADSL) for a specified ATM interface, use the **show dsl interface atm** command in user EXEC or privileged EXEC mode.

show dsl interface atm *interface-number*

Syntax Description

interface-number	(Optional) ATM interface number.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XJ	The command was introduced on Cisco 1700 series routers.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.1(5)YB	Support for this command was added to Cisco 2600 series and Cisco 3600 series routers.
12.1(5)XR1	Support for this command was added to the Cisco IAD2420 series.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Usage Guidelines

Use this command to display the status or results of a line test and to get information on port status, alarms, configured and actual transmission rates, and transmission errors. The **atm** word in this command is not a keyword but it is part of the command and optional. The output of this command is not affected by the **atm** keyword.

The output from this command appears the same as the output from the **show controller atm**command on Cisco 1400 series routers.

Examples

Examples

The following is sample output from the **show dsl interface atm** command for a CPE device that is configured for ADSL:

```
Router# show dsl interface atm 0/0
Alcatel 20150 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.1 (G.DMT)
ITU STD NUM:     0x01                            0x1
Vendor ID:       'ALCB'                          'ALCB'
Vendor Specific: 0x0000                          0x0000
Vendor Country:  0x00                            0x0F
Capacity Used:   85%                             98%
Noise Margin:    13.5 dB                          7.0 dB
Output Power:     9.5 dBm                        12.0 dBm
Attenuation:      1.5 dB                          3.5 dB
Defect Status:   None                            None
Last Fail Code:  None
Selftest Result: 0x00
Subfunction:     0x15
Interrupts:      5940 (0 spurious)
PHY Access Err:  0
Activations:     1
SW Version:      3.670
FW Version:      0x1A04
                 Interleave             Fast    Interleave             Fast
Speed (kbps):             0             8128             0              864
Reed-Solomon EC:          0                0             0                0
CRC Errors:               0                0             0                7
Header Errors:            0                0             0                2
Bit Errors:               0                0
BER Valid sec:            0                0
BER Invalid sec:          0                0
DMT Bits Per Bin
00: 0 0 0 0 0 0 0 7 6 7 9 A B C C C
10: C C C C C C B B B B A 9 A 9 0 0
20: 0 0 0 0 0 0 2 2 3 4 4 5 6 6 7 7
30: 7 8 8 8 9 9 9 A A A A A A B B B
40: B B B B B B B B B B B A B B B B
50: B B B B B B B B B B B B 2 B B B
60: B B B B B B B B B B B B B B B B
70: B B B B B B B B B B B B B B B B
80: B B B B B B B B B B B B B B B B
90: B B B B B B B B B B B B B B B B
A0: B B B B B B B B B B B B B B B B
B0: B B B B B B B B B B B B A B A A
C0: A A A A A A A A A A A A A A A A
D0: A A A A A A A A A A A 9 9 9 9 9
E0: 9 9 9 9 9 9 9 9 9 9 9 9 8 8 8 8
F0: 8 8 8 8 8 8 7 7 7 7 6 6 5 5 4 4
```

The table below describes the significant fields shown in the display.

Table 11: show dsl interface atm Field Descriptions

Field	Description
Modem Status	Status of the modem. Possible states include the following: DMTDSL_INVALID--Error state. DMTDSL_STOP--Administrative down state. DMTDSL_INIT--Restarting line. DMTDSL_CHK_HW--Confirming that required HW exists. DMTDSL_DLOAD_1--Downloading the init.bin file. DMTDSL_DLOAD_2--Downloading operational firmware. DMTDSL_MODE_CHK--Verifying that download was successful. DMTDSL_DO_OPEN--Issue ADSL_OPEN command. DMTDSL_RE_OPEN--Cycle the link. Retry open. DMTDSL_ACTIVATING--Waiting for activation to succeed. DMTDSL_LOOPBACK--Activation done. DMTDSL_SHOWTIME--Activation succeeded.
DSL Mode	DSL operating mode.
ITU STD NUM	ITU standard number for the operating mode.
Vendor ID	Vendor identification code.
Vendor Specific	Indicates if this router is specified for a vendor.
Vendor Country	Code for the country where the vendor is located.
Capacity Used	Percentage of the capacity that is being used.
Noise Margin	Noise margin, in decibels.
Output Power	Power output, in decibels.
Attenuation	Attenuation of the signal, in decibels.
Defect Status	Status of defects.
Last Fail Code	Last failure code that was logged.

Field	Description
Selftest Result	Results of the self-test.
Subfunction	Code for the subfunction running.
Interrupts	Code for interrupts used.
PHY Access Err	Number of physical access errors.
Activations	Number of activations of the router.
SW Version	Software version number.
FW Version	Firmware version number.
Speed	The train speed for upstream and downstream. It shows both the interleave and the fast mode.
Reed-Solomon EC	Reed-Solomon error-correction statistics.
CRC Errors	Cyclic redundancy check statistics.
Header Errors	ATM header error reports.
Bit Errors	Total number of bit errors.
BER Valid sec	Bit error rate valid seconds.
BER Invalid sec	Bit error rate invalid seconds.

Examples

The following is sample output from the **show dsl interface atm** command for a CPE device that is configured for G.SHDSL:

```
Router# show dsl interface atm 0/0
Globespan G.SHDSL Chipset Information
Equipment Type: Customer Premise
Operating Mode: G.SHDSL
Clock Rate Mode: Auto rate selection Mode
Reset Count: 1
Actual rate: 2320 Kbps
Modem Status: Data
Noise Margin: 42 dB
Loop Attenuation: 0.0 dB
Transmit Power: 13.5 dB
Receiver Gain: 204.8000 dB
Last Activation Status:No Failure
CRC Errors: 0
Chipset Version: 1
Firmware Version: R1.0
```

The table below describes the significant fields shown in the display.

Table 12: show dsl interface atm Field Descriptions

Field	Description
Equipment Type	Terminal type, which can be one of the following: • Customer Premise (CPE)--This value indicates that the device is connected to a DSLAM. This is the default. • Central Office (CO)--If the devices are connected back-to-back, one of the routers can act as a CO.
Operating Mode	G.SHDSL annex configuration, which can be one of the following values: • A--Operating parameters for North America. This value is the default. • B--Operating parameters for Europe.
Clock Rate Mode	Upstream and downstream bit rate configuration, in kb/s. If the upstream and downstream rates have different values, the device will train to lowest of the rates. If the value indicates "Auto Rate Selection Mode," the CO and CPE devices will negotiate the speed and train.
Reset Count	Number of times the G.SHDSL chip has been reset since powering up.
Actual rate	The actual bit rate that the transceiver is using. This rate could be different from the requested (configured) rate.
Modem Status	One of the following values: • Handshake--local transceiver is trying to reach the far-end transceiver. • Training--startup training is in progress. • Data--training was successful.
Received SNR	The received signal-to-noise ratio (SNR), in decibels (dB).
SNR Threshold	SNR threshold below which the router will retrain. The default is 23 dB.

Field	Description
Loop Attenuation	The difference in decibels between the power received at the near-end device and the power transmitted from the far-end device.
Transmit Power	Local STU transmit power, in decibels per milliwatt (dBm).
Receiver Gain	Total receiver gain.
Last Activation Status	Defines the last failure state of the G.SHDSL chip.
CRC Errors	Number of cyclic redundancy check (CRC) errors observed after bootup or resetting of the interface.
Chipset Version	Vendor’s chipset version.
Firmware Version	Version of the vendor’s chipset firmware.

Related Commands

Command	Description
dsl operating-mode	Modifies the operating mode of the digital subscriber line for an ATM interface.
show controller atm	Displays information about about an inverse multiplexing over ATM (IMA) group.

show ip http client cookie

To display the HTTP client cookies, use the **show ip http client cookie** command in privileged EXEC mode.

show ip http client cookie {**brief**| **summary**} [**domain** *cookie-domain*| **name** *cookie-name*| **session** *session-name*]

Syntax Description

brief	Displays a brief summary of client cookies.
summary	Displays a detailed summary of client cookies.
domain	(Optional) Displays all cookies in a domain
cookie-domain	(Optional) Client cookie domain or host name.
name	(Optional) Displays cookies matching a specific name.
cookie-name	(Optional) Client cookie name.
session	(Optional) Displays cookies specific to a client session.
session-name	(Optional) Client session name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is example output from the **show ip http client cookie brief**command:

```
Device# show ip http client cookie brief
HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7         7                               1       172.17.0.2
/cwmp-1-0/
cookie3         3                               1       172.16.0.2
/cwmp-1-0/
cookie2         2                               1       172.16.0.2
/cwmp-1-0/
```

```
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie brief domain**command:

```
Device# show ip http client cookie brief domain 172.16.0.2
HTTP client cookies of domain 172.16.0.2 :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief name**command:

```
Device# show ip http client cookie brief name cookie3
HTTP client cookies of name cookie3 :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie brief session**command:

```
Device# show ip http client cookie brief session CWMP_CLIENT
HTTP client cookies of session CWMP_CLIENT :
For expanded output please use 'summary' option for display
Name            Value                           Ver     Domain
Path
cookie8          8                              1       172.17.0.2
/cwmp-1-0/
cookie7          7                              1       172.17.0.2
/cwmp-1-0/
cookie3          3                              1       172.16.0.2
/cwmp-1-0/
cookie2          2                              1       172.16.0.2
/cwmp-1-0/
cookie1          1                              1       172.16.0.2
/cwmp-1-0/
```

The following is example output from the **show ip http client cookie summary**command:

```
Device# show ip http client cookie summary
HTTP client cookies of session HTTP CFS :
HTTP client cookies of session CWMP_CLIENT :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie3
```

```
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
HTTP client cookies of session cwmp_test_client :
```

The following is example output from the **show ip http client cookie summary domain**command:

```
Device# show ip http client cookie summary domain 172.17.0.2
HTTP client cookies of domain 172.17.0.2 :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary name**command:

```
Device# show ip http client cookie summary name cookie7
HTTP client cookies of name cookie7 :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

The following is example output from the **show ip http client cookie summary session**command:

```
Device# show ip http client cookie summary session CWMP_CLIENT
HTTP client cookies of session CWMP_CLIENT :
Name          : cookie8
Value         :  8
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie7
Value         :  7
Version       : 1
Domain        : 172.17.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :

Name          : cookie3
Value         :  3
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie2
Value         :  2
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
Name          : cookie1
Value         :  1
Version       : 1
Domain        : 172.16.0.2 (default)
Path          : /cwmp-1-0/ (default)
Secure        : no
Max-Age       : 600
Port          :
Comment       :
CommentURL    :
```

show mpf cpu

To display the average CPU utilization over a duration of the last 5 seconds, the last 1 minute, and the last 5 minutes when Multi-Processor Forwarding (MPF) is enabled on the second CPU, use the **show mpf cpu**command in user EXEC or privileged EXEC mode.

show mpf cpu [history]

Syntax Description

history	(Optional) Displays graphical output of the second CPU utilization over the last 60 seconds, the last 60 minutes, and the last 72 hours.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and supported on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Examples

The following example shows that the average utilization of the second CPU is 33 percent for the last 5 seconds, 25 percent for the last minute, and 30 percent for the last 5 minutes:

```
Router# show mpf cpu
CPU utilization for five seconds: 33%; one minute: 25%; five minutes: 30%
```

The following example shows graphical output of utilization of the second CPU for the last 60 seconds (percentage of CPU use per second), the last 60 minutes (percentage of CPU use per minute), and the last 72 hours (percentage of CPU use per hour).

```
Router# show mpf cpu history
slns 12:12:40 AM Saturday Nov 18 2000 UTC
3333333333333333333333333333333333333333333333333333333333
3333333333333333333333333333333333333333333333333333333333
100
90
80
70
60
50
40
30 ***************************
20 ***************************
10 ***************************
```

```
0....5....1....1....2....2....3....3....4....4....5....5....
     0     5     0    5     0     5    0    5    0    5
    CPU% per second (last 60 seconds)
3333333333333333333333333333333333333333333333333333333333
3333333333333333333333333333333333333333333333333333333333
100
90
80
70
60
50
40
30 #################
20 #################
10 #################
0....5....1....1....2....2....3....3....4....4....5....5....
    0     5    0     5     0     5    0     5    0     5
     CPU% per minute (last 60 minutes)
     * = maximum CPU% # = average CPU%
1
60
80
100 *
90 *
80 *
70 **
60 **
50 **
40 ##
30 ##
20 ##
10 ##
0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
    0         5     0    5    0    5    0    5    0    5    0    5    0
     CPU% per hour (last 72 hours)
     * = maximum CPU% # = average CPU%
```

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enable MPF on the second CPU of Cisco 7200 VXR and Cisco 7301 routers.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show mpf interface

To display Multi-Processor Forwarding (MPF) packet counter information on each physical interface, use the **show mpf interface**command in user EXEC or privileged EXEC mode.

show mpf interface [interface-name-and-number] [dot1q-vlan-num]

Syntax Description

interface-name-and-number	(Optional) Displays punt counts for a specified Gigabit Ethernet interface and its slot number and port number.
dotlq-vlan-num	(Optional) Displays punt counts on a specific subinterface by specifying the 802.1Q VLAN number.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

This command is supported for physical interfaces and subinterfaces. There is no support for the virtual access interface (VAI).

You can display the interface count information for a specific Gigabit Ethernet interface by specifying the interface name and number. To display interface information for a specified subinterface only, you must use the 802.1Q VLAN number for the subinterface because the MPF software does not recognize the subinterface number.

Using the show mpf interface command without arguments displays the interface information for all Gigabit Ethernet interfaces and subinterfaces.

Using the **clear mpf interface** command resets the interface packet counters shown in the **show mpf interface** command output.

Examples

The following example using the show mpf interface command without arguments displays interface information about up or down state, type of counter (receiving or transmitting packet or bytes), and count number for packets or bytes for all Gigabit Ethernet interfaces (only GigabitEthernet0/1 in this example) and subinterfaces:

```
Router# show mpf interface
Name           Index   State       Counter              Count
Gi0/1          0       up          RX packets           1004
                                   RX bytes             158632
                                   TX packets           5004
Name           Index  State        Counter              Count
                                   TX bytes             790632
                                   RX punts             32961
                                   TX punts             85972
Gi0/1          1      up
Gi0/1.100      100    up           RX packets           1004
                                   RX bytes             158632
                                   TX packets           5004
                                   TX bytes             790632
                                   RX punts             25
Gi0/1.101      101    up
Gi0/1.102      102    up
Gi0/1.105      105    up
Gi0/1.106      106    up
Gi0/1.107      107    up
Gi0/1.200      200    up
Gi0/1.201      201    up           RX punts             29
Gi0/1.202      202    up
Gi0/1.206      206    up
Gi0/1.2002     602    up           RX punts             26114
Gi0/1.2004     604    up
```

The following example specifies interface information for Gigabit Ethernet interface 0/1 subinterface 100. However, all Gigabit Ethernet interface and subinterface information is displayed because MPF does not recognize the subinterface number, unless it is a VLAN number.

```
Router# show mpf interface
GigabitEthernet0/1.100
Name          Index   State     Counter               Count
Gi0/1         0       up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
                                TX bytes              790632
                                RX punts              32996
                                TX punts              86062
Gi0/1         1       up
Gi0/1.100     100     up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
                                TX bytes              790632
                                RX punts              25
Gi0/1.101     101     up
Gi0/1.102     102     up
Gi0/1.105     105     up
Gi0/1.106     106     up
Gi0/1.107     107     up
Gi0/1.200     200     up
Gi0/1.201     201     up       RX punts               29
Gi0/1.202     202     up
Gi0/1.206     206     up
Gi0/1.2002    602     up       RX punts               26142
Gi0/1.2004    604     up
```

The following example displays the interface information for VLAN number 100 on Gigabit Ethernet interface 0/1, including up state, receiving packet count, receiving bytes count, transmitting packet count, transmitting byte count, and receiving punt count:

```
Router# show mpf interface GigabitEthernet0/1 100
```

```
Name          Index   State     Counter               Count
Gi0/1.100     100     up        RX packets            1004
                                RX bytes              158632
                                TX packets            5004
                                TX bytes              790632
                                RX punts              25
```

The table below describes the fields shown in the output examples.

Table 13: show mpf interface Field Descriptions

Field	Description
Name	Gigabit Ethernet interface name and number.
Index	This is for internal use and can be ignored.
State	Up or down state of interface.
Counter	Type of counter.
Count	Number of packets or bytes.
RX packets	Packets received through the Gigabit Ethernet interface and processed by the second CPU, CPU1. These packets are MPF accelerated.
RX bytes	Bytes received and processed by the second CPU, CPU1.
RX punts	Packets received through the Gigabit Ethernet interface and punted by the second CPU, CPU1, to CPU0 for Cisco IOS processing.
RX drop	Packets received through the Gigabit Ethernet interface but dropped by the second CPU, CPU1.
TX packets	MPF accelerated packets transmitted from the Gigabit Ethernet interface using the second CPU, CPU1.
TX bytes	Bytes transmitted by the second CPU, CPU1.
TX punts	Packets transmitted from the second CPU, CPU1. Packets that have been punted to CPU0 and processed by Cisco IOS software are redirected to CPU1 for transmitting from the relevant Gigabit Ethernet interface.
TX drop	Packets that were dropped by the second CPU, CPU1, while in the process of being transmitted from the Gigabit Ethernet interface.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show mpf ip exact-route

To display the exact route for a source-destination address IP pair in a Multi-Processor Forwarding (MPF) system, use the **show mpf ip exact-route**command in user EXEC or privileged EXEC mode.

show mpf ip exact-route [**vrf vrf-name**] **src-ip-addr dst-ip-addr**

Syntax Description

vrf	(Optional) A Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
src-ip-addr	Specifies the network source address.
dst-ip-addr	Specifies the network destination address.

Command Default

No default behavior or values.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and supported on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

When you are load balancing per destination, this command shows the exact next hop that is used for a given IP source-destination pair.

Examples

The following sample output displays the exact next hop (10.1.104.1) for the specified source IP address (10.1.1.1) and destination IP address (172.17.249.252):

```
Router# show mpf ip exact-route 10.1.1.1 172.17.249.252
10.1.1.1        -> 172.17.249.252 :GigabitEthernet2/0 (next hop 10.1.104.1)
```

The table below describes the significant fields shown in the output example.

Table 14: show mpf ip exact-route Field Descriptions

Field	Description
10.1.1.1 -> 172.17.249.252	From source 10.1.1.1 IP address to destination IP address 172.17.249.252.
GigabitEthernet2/0 (next hop 10.1.104.1)	Next hop is 10.1.104.1 on GigabitEthernet interface 2/0.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show mpf punt

To display the Multi-Processor Forwarding (MPF) punt reason and punt packet count for the chassis, use the **show mpf punt**command in user EXEC or privileged EXEC mode.

show mpf punt

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

The punt reason and punt packet count are collected for each box or chassis, not for each interface. Packets that are punted are directed for Cisco IOS processing and are not accelerated by MPF.

Examples

The following example displays the types of packet, the reasons for the punt, and the punt packet counts for the router chassis.

```
Router# show mpf punt
  Type     Message         Count
  l2tp     unknown session errors          7
  l2tp     L2TP control          6
  ipv4/verify     adjacency punt          1
  ethernet     unknown ethernet type             542
  ppp     punts due to unknown protocol    333
  arp     ARP request          6
```

The table below describes the fields in the **show mpf punt** output display.

Table 15: show mpf punt Field Descriptions

Field	Description
Type	Packet type or encapsulation, such as ARPA, Ethernet, or L2TP.
Message	Reason for punting the packet to Cisco IOS processing.
Count	Punt packet count.

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
sw-module heap fp	Fine-tunes the MPF heap memory allocation.

show ppp interface

To display the IP Control Protocol (IPCP) and Link Control Protocol (LCP) information for all the sessions on an ATM or Gigabit Ethernet interface, use the **show ppp interface** command in user EXEC or privileged EXEC mode.

show ppp interface *interface number*

Syntax Description

interface number	Specifies a particular ATM or Gigabit Ethernet interface and the interface number.

Command Modes

User EXEC (>) Privileged EXEC (#))

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.
Cisco IOS Release 15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show ppp interface**command is used to display IPCP and LCP information for all the sessions on an ATM or Gigabit Ethernet interface.

Examples

The following example displays the IPCP and LCP information on the Gigabit Ethernet interface. The output is self-explanatory.

```
Device# show ppp interface GigabitEthernet 0/1/0.101

Gi0/1/0.101 No PPP serial context
PPP Session Info
----------------
Interface        : Vi2.1
PPP ID           : 0x26000001
Phase            : UP
Stage            : Local Termination
Peer Name        : user_01@domain_3
Peer Address     : 12.0.0.1
Control Protocols: LCP[Open] CHAP+ IPCP[Open]
Session ID       : 1
AAA Unique ID    : 12
SSS Manager ID   : 0x25000003
SIP ID           : 0x7B000002
PPP_IN_USE       : 0x15

Vi2.1 LCP: [Open]
Our Negotiated Options
Vi2.1 LCP:    MRU 1492 (0x010405D4)
```

```
Vi2.1 LCP:    AuthProto CHAP (0x0305C22305)
Vi2.1 LCP:    MagicNumber 0x21F4CD31 (0x050621F4CD31)
Peer's Negotiated Options
Vi2.1 LCP:    MRU 1492 (0x010405D4)
Vi2.1 LCP:    MagicNumber 0x4A51A20E (0x05064A51A20E)

Vi2.1 IPCP: [Open]
Our Negotiated Options
Vi2.1 IPCP:    Address 10.0.0.1 (0x03060A000001)
Peer's Negotiated Options
Vi2.1 IPCP:    Address 12.0.0.1 (0x03060C000001)
Device# show ppp interface atm 3/0.2

 AT3/0.2 No PPP serial context
 PPP Session Info
 ----------------
 Interface        : Vi2.1
 PPP ID           : 0x3A000001
 Phase            : UP
 Stage            : Local Termination
 Peer Name        : joe@pepsi.com
 Peer Address     : 20.21.22.23
 Control Protocols: LCP[Open] PAP+ IPCP[Open]
 Session ID       : 1
 AAA Unique ID    : 12
 SSS Manager ID   : 0x40000003
 SIP ID           : 0x86000002
 PPP_IN_USE       : 0x15

 Vi2.1 LCP: [Open]
 Our Negotiated Options
 Vi2.1 LCP:    MRU 1492 (0x010405D4)
 Vi2.1 LCP:    AuthProto PAP (0x0304C023)
 Vi2.1 LCP:    MagicNumber 0x06545BB4 (0x050606545BB4)
 Peer's Negotiated Options
 Vi2.1 LCP:    MRU 1492 (0x010405D4)
 Vi2.1 LCP:    MagicNumber 0x01CB46A9 (0x050601CB46A9)

 Vi2.1 IPCP: [Open]
 Our Negotiated Options
   NONE
 Our Rejected options
   Address
 Peer's Negotiated Options
 Vi2.1 IPCP:    Address 20.21.22.23 (0x030614151617)
```

Related Commands

Command	Description
ppp bap	Displays the BAP configuration settings and run-time status for a multilink bundle.
ppp queues	Monitors the number of requests processed by each AAA background process.

show ppp subscriber statistics

To display PPP subscriber statistics, use the **show ppp subscriber statistics** command in privileged EXEC mode.

show ppp subscriber statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is useful for obtaining events and statistics for PPP subscribers. Use the show ppp subscriber statistics command to display a cumulative count of PPP subscriber events and statistics, and to display an incremental count since the clear ppp subscriber statistics command was last issued.

Examples

The following is sample output from the show ppp subscriber statistics command:

```
Router# show ppp subscriber statistics
PPP Subscriber Events          TOTAL         SINCE CLEARED
Encap                          32011         32011
DeEncap                        16002         16002
CstateUp                       173           173
CstateDown                     36            36
FastStart                      0             0
LocalTerm                      7             7
LocalTermVP                    0             0
MoreKeys                       173           173
Forwarding                     0             0
Forwarded                      0             0
SSSDisc                        0             0
SSMDisc                        0             0
PPPDisc                        167           167
PPPBindResp                    173           173
PPPReneg                       3             3
RestartTimeout                 169           169
>
PPP Subscriber Statistics      TOTAL         SINCE CLEARED
IDB CSTATE UP                  16008         16008
IDB CSTATE DOWN                40            40
APS UP                         0             0
APS UP IGNORE                  0             0
APS DOWN                       0             0
READY FOR SYNC                 10            10
```

The table below describes the significant fields shown in the display. Any data not described in the table below is used for internal debugging purposes.

Table 16: show ppp subscriber statistics Field Descriptions

Field	Description
PPP Subscriber Events	PPP subscriber event counts.
Encap	Number of times PPP encapsulation occurred.
DeEncap	Number of times PPP deencapsulation occurred.
CstateUp	Number of times PPP interfaces were initialized.
CstateDown	Number of times PPP interfaces were shut down.
FastStart	Number of PPP sessions started by link control protocol (LCP) packets before the interface state was up.
LocalTerm	Number of locally terminated PPP sessions.
LocalTermVP	Number of locally terminated PPP sessions running on virtual profiles.
MoreKeys	Number of PPP sessions in the intermediate state--that is, processing service keys--before a session is forwarded or terminated locally.
Forwarding	Number of PPP sessions in forwarding state.
Forwarded	Number of PPP sessions that have been forwarded.
SSSDisc	Number of PPP sessions disconnected from the subscriber service switch after receiving a disconnect notification.
SSMDisc	Number of PPP sessions disconnected from the dataplane after receiving a disconnect notification.
PPP BindResp	Number of PPP responses where the interface has been bound to the session.
PPP Reneg	Number of PPP renegotiation events.
RestartTimeout	Occurrences of the restart timer beginning on PPP encapsulated interfaces in the down state.
PPP Subscriber Statistics	PPP subscriber statistic counts.
IDB CSTATE UP	Occurrences of the IDB making the transition to the up state.

Field	Description
IDB CSTATE DOWN	Occurrences of the IDB making the transition to the down state.
APS UP	Occurrences of PPP sessions receiving automatic protection switching (APS) selected events.
APS UP IGNORE	Occurrences of PPP sessions receiving APS selected events when the IDB state was down.
APS DOWN	Occurrences of PPP sessions receiving APS deselected events.
READY FOR SYNC	Number of PPP sessions ready for synchronization.

Related Commands

Command	Description
clear ppp subscriber statistics	Clears PPP subscriber statistics.

show pppatm redundancy

To display PPP over ATM (PPPoA) statistics, use the **show pppatm** redundancy command in privileged EXEC mode.

show pppatm redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is useful for obtaining statistics for PPPoA sessions. This command gives a total count of PPPoA events since the clear pppatm statistics command was last issued.

Examples

The following is sample output from the **show pppatm redundancy** command:

```
Router# show pppatm redundancy
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

Table 17: show pppatm redundancy Field Descriptions

Field	Description
SSS request events	Subscriber service switch (SSS) requests.

Field	Description
SSS Msg events	SSS responses
PPP Msg events	PPP responses.
Up Pending events	ATM VC notification of events in queue.
Up dequeued events	ATM VC notification of events removed from queue.
Processing Up events	PPPoA events processed.
Vaccess Up events	Number of events for which the virtual access interface state changed to up.
AAA unique id allocated events	Number of events for which a unique AAA ID was allocated.
No AAA method list set events	Number of events for which no AAA accounting list was configured.
AAA get NAS port details events	Number of NAS port events.
AAA gets retrieved attrs events	Number of AAA retrieved attributes events for incoming and outgoing packets.
AAA gets dynamic attrs events	Number of AAA dynamic attributes events for start/stop packets.
Access IE allocated events	Number of IE (internal ID) allocated events.

Related Commands

Command	Description
show pppatm statistics	Displays PPP ATM statistics.
show pppoe redundancy	Displays PPPoE events and statistics.

show pppatm session

To display information on PPP over ATM (PPPoA) sessions, use the **show pppatm session** command in privileged EXEC mode.

show pppatm session[**interface atm** *interface-number.sub-interface number*]

Syntax Description

interface atm	(Optional) Configures an ATM interface.
interface-number.subinterface-number	Interface number and possibly a subinterface number. A period (.) must precede the optional subinterface number.

Command Default

If no keywords or arguments are provided, information for all PPPoA sessions is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is used for obtaining detailed information on PPPoA sessions, and the interfaces on which they are running.

If a subinterface number is given in the command, the output is a report of the PPPoA sessions in the subinterface. If a main interface number is given, the output has the report for each individual subinterface of that main interface. If no interface is given, the output contains the report for each ATM interface on the router.

Examples

The following example shows how to display information for PPPoA sessions on ATM interface 8/0/0.12345678:

```
Router# show pppatm session atm8/0/0.12345678
     1 session  in LCP_NEGOTIATION (LCP) State
     1 session  total
Uniq ID  ATM-Intf       VPI/VCI   Encap   VT  VA         VA-st  State
8001 8/0/0.12345678 0/32035 SNAP 10 N/A N/A LCP
```

The table below describes the significant fields shown in the display.

Table 18: show pppatm session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoA session.
ATM-Intf	The ATM interface port number.
VPI	Virtual path identifier of the permanent virtual circuit (PVC).
VCI	Virtual channel identifier of the PVC.
Encap	Number of times PPP encapsulation occurred.
VT	Virtual template number used by the session.
VA	Virtual access interface number.
VA-st	Virtual access interface state.
State	PPPoA state of the session.

Related Commands

Command	Description
show pppatm summary	Displays PPPoA session counts

show pppatm statistics

To display PPP over ATM (PPPoA) statistics, use the **show pppatm statistics** command in privileged EXEC mode.

show pppatm statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **show pppatm statistics**command to display statistics for PPPoA sessions. This command gives a total count of PPPoA events since the **clear pppatm statistics** command was last issued.

Examples

The following is sample output from the **show pppatm statistics** command:

```
Router# show pppatm statistics
 4000 : Context Allocated events
 3999 : SSS Request events
 7998 : SSS Msg events
 3999 : PPP Msg events
 3998 : Up Pending events
 3998 : Up Dequeued events
 3998 : Processing Up events
 3999 : Vaccess Up events
 3999 : AAA unique id allocated events
 3999 : No AAA method list set events
 3999 : AAA gets nas port details events
 3999 : AAA gets retrived attrs events
 68202 : AAA gets dynamic attrs events
 3999 : Access IE allocated events
```

The table below describes the significant fields shown in the display.

Table 19: show pppatm statistics Field Descriptions

Field	Description
Context Allocated events	Number of PPPoA events for which a context has been allocated.
SSS Request events	Subscriber service switch (SSS) requests.

Field	Description
SSS Msg events	SSS responses.
PPP Msg events	PPP responses.
Up Pending events	ATM VC notification of events in queue.
Up Dequeued events	ATM VC notification of events removed from queue.
Processing Up events	PPPoA events processed.
Vaccess Up events	Number of events for which the virtual access interface state changed to up.
AAA unique id allocated events	Number of events for which a unique authentication, authorization, and accounting (AAA) ID was allocated.
No AAA method list set events	Number of events for which no AAA accounting list was configured.
AAA get nas port details events	Number of network accesss server (NAS) port events.
AAA gets retrieved attrs events	Number of AAA retrieved attributes events for incoming and outgoing packets.
AAA gets dynamic attrs events	Number of AAA dynamic attributes events for start/stop packets.
Access IE allocated events	Number of IE (internal ID) allocated events.

Related Commands

Command	Description
clear pppatm statistics	Clears PPP ATM statistics.

show pppatm summary

To display PPP over ATM (PPPoA) session counts, use the **show pppatm summary** command in privileged EXEC mode.

show pppatm summary [**interface atm** *interface-number* [. *subinterface-number*]]

Syntax Description

interface atm *interface-number* **.** *subinterface-number*	(Optional) Specifies a particular ATM interface by interface number and possibly a subinterface number. A period (**.**) must precede the optional subinterface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command is useful for obtaining session counts, the state of the PPPoA sessions, and the interfaces on which they are running.

This command gives a summary of the number of PPPoA sessions in each state and the session information of each individual session. If a subinterface number is given in the command, the output is a summary report of the PPPoA sessions in the subinterface. If a main interface number is given, the output will have the summary reports for each individual subinterface of that main interface as shown in the Examples section. If no interface is given, the output will contain the summary reports for each ATM interface on the router.

Examples

The following example displays PPPoA session counts and states for ATM interface 5/0:

```
Router# show pppatm summary interface atm 5/0
ATM5/0.3:
       0 sessions total
ATM5/0.6:
       1 in PTA (PTA) State
       1 sessions total
VPI     VCI     Conn ID         PPPoA ID        SSS ID          PPP ID        AAA ID   VT
     VA/SID  State
  6     101       11            DA000009       BB000013       E5000017        C        1
     1.1     PTA
```

Most of the fields displayed by the **show pppatm summary** command are self-explanatory. The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

Table 20: show pppatm summary Field Descriptions

Field	Description
VPI	Virtual path identifier of the permanent virtual circuit (PVC).
VCI	Virtual channel identifier of the PVC.
Conn ID	Unique connection identifier for the PPPoA session. This ID can be correlated with the unique ID in the **show vpdn session** command output for the forwarded sessions.
PPPoA ID	Internal identifier for the PPPoA session.
SSS ID	Internal identifier in the Subscriber Service Switch.
PPP ID	Internal identifier in PPP.
AAA ID	Authentication, authorization, and accounting (AAA) unique identifier for accounting records.
VT	Virtual template number used by the session.
VA/SID	PPPoA virtual access number for PPP Termination Aggregation (PTA) sessions, and switch identifier for forwarded sessions.
State	PPPoA state of the session.

Related Commands

Command	Description
clear pppatm interface atm	Clears PPP ATM sessions on an ATM interface.
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.
show pppatm trace	Displays a sequence of PPPoA events, errors, and state changes when the **debug pppatm** command is enabled.

show ppp atm trace

To display a sequence of PPP over ATM (PPPoA) events, errors, and state changes when the **debug pppatm** command is enabled, use the **show pppatm trace** command in privileged EXEC mode.

show pppatm trace [**error**| **event**| **state**] **interface atm** *interface-number* [[*.subinterface-number*]] **vc** {[*vpi*]/ *vci*| **virtual-circuit-name**}

Syntax Description

error	(Optional) PPPoA events.
event	(Optional) PPPoA errors.
state	(Optional) PPPoA state.
interface atm *interface-number*	Specifies a particular ATM interface by interface number.
. *subinterface-number*	(Optional) Specifies a subinterface number preceded by a period.
show pppatm trace [**error**| **event**| **state**] **interface atm** *interface-number* [[*.subinterface-number*]] **vc** {[*vpi*]/ *vci*| **virtual-circuit-name**} **vc** *vpi* / *vci*	Virtual circuit (VC) keyword followed by a virtual path identifier (VPI) and virtual channel identifier (VCI). The absence of the "/" and a *vpi* causes the *vpi* value to default to 0.
virtual-circuit-name	Name of the VC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When the **debug pppatm** command has been enabled, this command displays messages from the specified permanent virtual circuit (PVC). If only one **debug pppatm** command keyword is supplied in the command, the report will display only the sequence of events for that particular debug type.

Examples

The following example traces the debugging messages supplied by the **debug pppatm** command on PVC 101. The report is used by Cisco technical personnel for diagnosing system problems.

```
Router# debug pppatm trace interface atm 1/0.10 vc 101
Router# debug pppatm state interface atm 1/0.10 vc 101
Router# debug pppatm event interface atm 1/0.10 vc 101
Router# show pppatm trace interface atm 1/0.10 vc 101
Event = Disconnecting
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = SSS Cleanup
State = DOWN
Event = Up Pending
Event = Up Dequeued
Event = Processing Up
Event = Access IE allocated
Event = Set Pkts to SSS
Event = AAA gets retrieved attrs
Event = AAA gets nas port details
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = AAA unique id allocated
Event = No AAA method list set
Event = SSS Request
State = NAS_PORT_POLICY_INQUIRY
Event = SSS Msg
State = PPP_START
Event = PPP Msg
State = LCP_NEGOTIATION
Event = PPP Msg
Event = Access IE get nas port
Event = AAA gets dynamic attrs
Event = AAA gets dynamic attrs
Event = PPP Msg
Event = Set Pkts to SSS
State = FORWARDED
```

Related Commands

Command	Description
clear pppatm interface atm	Clears PPP ATM sessions on an ATM interface.
debug pppatm	Enables reports for PPPoA events, errors, and states either globally or conditionally on an interface or VC.
show pppatm summary	Displays PPPoA session counts.

show pppoe debug conditions

To display PPP over Ethernet (PPPoE) debug information, use the **show pppoe debug conditions** command in user EXEC or privileged EXEC mode.

show pppoe debug conditions

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show pppoe debug conditions** command. The fields in the display are self-explanatory.

```
Router# show pppoe debug conditions
PPPoE global debugs: packet
AT6/0 debugs: event, error
AT6/0, VC 1/100 debugs: data
```

Related Commands

Command	Description
clear pppoe	Clears PPPoE sessions.
debug pppoe	Displays debugging information for PPPoE sessions.
show pppoe session	Displays information about currently active PPPoE sessions.

show pppoe derived

To display the cached PPP over Ethernet (PPPoE) configuration that is derived from the subscriber profile for a specified PPPoE profile, use the **show pppoe derived** command in privileged EXEC mode.

show pppoe derived group *group-name*

Syntax Description

group *group-name*	PPPoE profile for which the cached PPPoE configuration will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

A subscriber profile can be configured locally on the router or remotely on a AAA server. The PPPoE configuration that is derived from a subscriber profile is cached locally under the PPPoE profile. Use the **show pppoe derived**command to display the cached PPPoE configuration that is derived from the subscriber profile for a specified PPPoE profile.

A subscriber profile contains a list of PPPoE service names. The PPPoE server will advertise the service names that are listed in the subscriber profile to each PPPoE client connection that uses the configured PPPoE profile. A subscriber profile is assigned to a PPPoE profile by using the **service profile** command in BBA group configuration mode.

Examples

The following example shows the PPPoE configuration for PPPoE profile "sp_group_a" that is derived from subscriber profile "abc". The services "isp_xyz", "isp_aaa", and "isp_bbb" will be advertised to each PPPoE client connection that uses PPPoE profile "sp_group_a".

```
Router# show pppoe derived group sp_group_a
Derived configuration from subscriber profile 'abc':
Service names:
   isp_xyz, isp_aaa, isp_bbb
```

Related Commands

Command	Description
clear pppoe derived	Clears the cached PPPoE configuration of a PPPoE profile and forces the PPPoE profile to reread the configuration from the assigned subscriber profile.

Command	Description
pppoe service	Adds a PPPoE service name to a local subscriber profile.
service profile	Assigns a subscriber profile to a PPPoE profile.
subscriber profile	Defines Subscriber Service Switch policy for searches of a subscriber profile database.

show pppoe redundancy

To display PPP over Ethernet (PPPoE) redundancy events and statistics, use the **show pppoe redundancy** command in privileged EXEC mode.

show pppoe redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

This command is useful for obtaining statistics and redundancy events for PPPoE sessions such as recreating UP and DOWN states, and number of sessions waiting for an ATM virtual circuit to turn active. This command gives a cumulative count of PPPoE redundancy queue events and statistics, and an incremental count of PPPoE redundancy queue events and statistics since the last time the clear pppoe redundancy command was issued.

The **show pppoe redundancy** command does not show any output on an active Route Processor but shows output only on a standby Route Processor.

Examples

The following is sample output for the show pppoe redundancy command:

Examples

```
Router# show pppoe redundancy

11 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 Event Names
                          Events  Queued  MaxQueued  Suspends  usec/evt max/evt
Router#
```

Examples

```
Router-stby# show pppoe redundancy
13 Event Queues
                 size   max      kicks     starts    false   suspends  ticks(ms)
 9 PPPoE CCM EV     0    36       1524       1525        1          0        20
 Event Names
                           Events  Queued  MaxQueued  Suspends  usec/evt max/evt
 1* 9 Recreate UP           32000        0       36        0        93      2000
 2* 9 Recreate DOWN             0        0        0        0         0         0
 3* 9 VC Wait UP                0        0        0        0         0         0
 4* 9 VC Wait Encap             0        0        0        0         0         0
Sessions waiting for Base Vaccess: 0
Sessions waiting for ATM VC UP:    0
Sessions waiting for Auto VC Encap 0
```

The table below describes the significant fields in the sample output.

Table 21: show pppoe redundancy Field Descriptions

Field	Description
size	
max	
kicks	
starts	
false	
suspends	
ticks	
Events	
Queued	
MaxQueued	
Suspends	
usec/evt	
max/evt	

Related Commands

Command	Description
show pppoe statistics	Displays PPPoE statistics.

show pppoe relay context all

To display PPP over Ethernet (PPPoE) relay contexts created for relaying PPPoE Active Discovery (PAD) messages, use the **show pppoe relay context all** command in privileged EXEC mode.

show pppoe relay context all

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to display relay contexts created for relaying PAD messages.

Examples

The following is sample output from the **show pppoe relay context all** command:

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

The table below describes the significant fields shown in the show pppoe relay context all command output.

Table 22: show pppoe relay context all Field Descriptions

Field	Description
Total PPPoE relay contexts	PPPoE relay contexts created for relaying PAD messages.
UID	Unique identifier for the relay context.
ID	PPPoE session identifier for the relay context.
Subscriber-profile	Name of the subscriber profile that is used by the PPPoE group associated with the relay context.

Field	Description
State	Shows the state of the relay context, which will be one of the following: • INVALID--Not valid. • RELFWD--PPPoE relay context was forwarded. • REQ_RELAY--Relay has been requested.

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created by PAD messages.
show pppoe session	Displays information about currently active PPPoE sessions.

show pppoe session

To display information about currently active PPP over Ethernet (PPPoE) sessions, use the **show pppoe session** in privileged EXEC mode.

show pppoe session [**all** | **interface** *type number* | **packets** [**all**| **interface** *type number*| **ipv6**]]

Syntax Description

all	(Optional) Displays detailed information about the PPPoE session.
interface *type number*	(Optional) Displays information about the interface on which the PPPoE session is active.
packets	(Optional) Displays packet statistics for the PPPoE session.
ipv6	(Optional) Displays PPPoE session packet statistics for IPv6 traffic

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YG	This command was introduced on the Cisco SOHO 76, 77, and 77H routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted.
12.4(15)XF	The output was modified to display Virtual Multipoint Interface (VMI) and PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks (MANETs).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Release	Modification
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 3.5S	This command was modified. The **ipv6** keyword was added.

Examples

The following is sample output from the show pppoe session command:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st
26	19	0001.96da.a2c0	Et0/0.1	5	N/A	RELFWD	000c.8670.1006	VLAN:3434

Examples

The following is sample output from the **show pppoe session** command when there is an IWF session and the ppp-max-payload tag is accepted in the discovery frame (available in Cisco IOS Release 12.2(31)SB2):

```
Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total.  1 session of it is IWF type
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st	Type
26	21	0001.c9f2.a81e	Et1/2	1	Vi2.1	PTA	0006.52a4.901e	UP	IWF

The table below describes the significant fields shown in the displays.

Table 23: show pppoe session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoE session.
PPPoE SID	PPPoE session identifier.
RemMAC	Remote MAC address.
Port	Port type and number.
VT	Virtual-template interface.
VA	Virtual access interface.

Field	Description
State	Displays the state of the session, which will be one of the following: • FORWARDED • FORWARDING • LCP_NEGOTIATION • LOCALLY_TERMINATED • PPP_START • PTA • RELFWD (a PPPoE session was forwarded for which the Active discovery messages were relayed) • SHUTTING_DOWN • VACCESS_REQUESTED
LocMAC	Local MAC address.

Examples

The following example shows information per session for the **show pppoe session all** command.

```
Router# show pppoe session all

Total PPPoE sessions 1
session id: 21
local MAC address: 0006.52a4.901e, remote MAC address: 0001.c9f2.a81e
virtual access interface: Vi2.1, outgoing interface: Et1/2, IWF
PPP-Max-Payload tag: 1500
    15942 packets sent, 15924 received
    224561 bytes sent, 222948 received
```

Examples

The following example shows the output from the **show pppoe session all** command. This version of the display includes PPPoE credit flow statistics for the session.

```
Router# show pppoe session all
Total PPPoE sessions 1
session id: 1
local MAC address: aabb.cc00.0100, remote MAC address: aabb.cc00.0200
virtual access interface: Vi2, outgoing interface: Et0/0
17 packets sent, 24 received
1459 bytes sent, 2561 received
PPPoE Flow Control Stats
Local Credits: 65504 Peer Credits: 65478
Credit Grant Threshold: 28000 Max Credits per grant: 65534
PADG Seq Num: 7 PADG Timer index: 0
PADG last rcvd Seq Num: 7
PADG last nonzero Seq Num: 0
PADG last nonzero rcvd amount: 0
PADG Timers: [0]-1000 [1]-2000 [2]-3000 [3]-4000
PADG xmit: 7 rcvd: 7
PADC xmit: 7 rcvd: 7
PADQ xmit: 0 rcvd: 0
```

Examples

The following is sample output form the **show pppoe session packet ipv6** command. The output field descriptions are self-explanatory.

```
Device# show pppoe session packet ipv6

SID     Pkts -In         Pkts-Out        Bytes-In        Bytes-Out
1       2800            9               2721600         770
```

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created for relaying PAD messages.
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.

show pppoe statistics

To display PPP over Ethernet (PPPoE) events and statistics, use the **show pppoe statistics** command in privileged EXEC mode.

show pppoe statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is useful for obtaining statistics and events for PPPoE sessions. Use the show pppoe statistics command to display a cumulative count of PPPoE events and statistics, and to display an incremental count since the last time the clear pppoe statistics command was issued.

Examples

The following is sample output from the show pppoe statistics command:

```
Router# show pppoe statistics
PPPoE Events                   TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
INVALID                        0             0
PRE-SERVICE FOUND              0             0
PRE-SERVICE NONE               0             0
SSS CONNECT LOCAL              16002         16002
SSS FORWARDING                 0             0
SSS FORWARDED                  0             0
SSS MORE KEYS                  16002         16002
SSS DISCONNECT                 0             0
CONFIG UPDATE                  0             0
STATIC BIND RESPONSE           16002         16002
PPP FORWARDING                 0             0
PPP FORWARDED                  0             0
PPP DISCONNECT                 0             0
PPP RENEGOTIATION              0             0
SSM PROVISIONED                16002         16002
SSM UPDATED                    16002         16002
SSM DISCONNECT                 0             0
>
PPPoE Statistics               TOTAL         SINCE CLEARED
------------------------------ ------------- -------------
SSS Request                    16002         16002
SSS Response Stale             0             0
SSS Disconnect                 0             0
PPPoE Handles Allocated        16002         16002
PPPoE Handles Freed            0             0
```

```
Dynamic Bind Request           16002         16002
Static Bind Request            16002         16002
```

The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

Table 24: show pppoe statistics Field Descriptions

Field	Description
INVALID	Errors in the segment handling state machine; this field typically displays a zero.
PRE-SERVICE FOUND	Number of occurrences of PPPoE service policy having been located and configuration data having been read from the external server to the bba-group profile.
PRE-SERVICE NONE	Number of failures of PPPoE service policy profile configuration read from the external server.
SSS CONNECT LOCAL	Subscriber service switch (SSS) connections that received loca l termination directives.
SSS FORWARDING	SSS connections that received forwarding notification.
SSS FORWARDED	SSS connections that received forwarded notification.
SSS MORE KEYS	PPPoE sessions that are in the intermediate state, processing service keys, before a session is forwarded or terminated locally.
SSS DISCONNECT	PPPoE sessions disconnected after receiving a disconnect notification from the subscriber service switch.
CONFIG UPDATE	PPPoE sessions receiving serving policy configuration updates.
STATIC BIND RESPONSE	Number of responses that the interface is bound to the PPP session.
PPP FORWARDING	Number of PPPoE sessions in the forwarding state.
PPP FORWARDED	Number of forwarded PPPoE sessions.
PPP DISCONNECT	PPPoE sessions disconnected after receiving a disconnect message from the state machine.
PPP RENEGOTIATION	PPPoE sessions renegotiated after receiving a renegotiation message from the state machine.

Field	Description
SSM PROVISIONED	Segment switching manager (SSM) response that the dataplane has been initialized.
SSM UPDATED	SSM response that the dataplane has been successfully updated.
SSM DISCONNECT	Dataplane disconnects from PPPoE sessions.
SSS Request	SSS requests to determine if a call is to be forwarded or locally terminated.
SSS Response Stale	SSS responses received for sessions that are already freed.
SSS Disconnect	SSS disconnect messages to PPPoE sessions.
PPPoE Handles Allocated	Handles assigned for PPPoE sessions.
PPPoE Handles Freed	Handles freed for PPPoE sessions.
Dynamic Bind Request	PPPoE requests to start PPP sessions.
Static Bind Request	PPPoE requests to bind interfaces to PPP sessions.

Related Commands

Command	Description
clear pppoe statistics	Clears PPPoE statistics.

show pppoe summary

To display a summary of the currently active PPP over Ethernet (PPPoE) sessions per interface, use the **show pppoe summary** command in user EXEC or privileged EXEC mode.

show pppoe summary [**per subinterface**]

Syntax Description

per subinterface	(Optional) Displays the PPPoE sessions per subinterface.

Command Default

If no argument is specified, information for all PPPoE sessions is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show pppoe summary** command:

```
Router# show pppoe summary
PTA   Locally terminated sessions
    FWDED Forwarded sessions
    TRANS All other sessions (in transient state)
                    TOTAL     PTA   FWDED   TRANS
TOTAL                1762    1749      11       2
ATM2/0               1453    1443       8       2
ATM4/0                309     306       3       0
```

The table below describes the significant fields shown in the display.

Table 25: show pppoe summary Field Descriptions

Field	Description
TOTAL	Total number of sessions.

Field	Description
PTA	Total number of PPP Terminated Aggregation (PTA) sessions.
FWDED	Total number of sessions that are forwarded.
TRANS	Total number of sessions transmitted.

Related Commands

Command	Description
clear pppoe	Clears PPPoE sessions.
debug pppoe	Displays debugging information for PPPoE sessions.
show pppoe session	Displays information about currently active PPPoE sessions.

show pppoe throttled mac

To display information about MAC addresses from which PPP over Ethernet (PPPoE) sessions are throttled, that is, not currently accepted**, use the show pppoe throttled mac command**in privileged EXEC mode**.**

show pppoe throttled mac

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB4A	This command was introduced.
12.2(28)SB6	This command was integrated into Cisco IOS Release 12.2(28)SB6.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

PPPoE connection throttling limits the number of PPPoE session requests that can be made from a MAC address within a specified period of time. Use the show pppoe throttled mac command to display MAC addresses and ingress ports of users that exceed connection throttling limits configured using the sessions throttle command.

Examples

The following is sample output from the show pppoe throttled mac command:

```
Router# show pppoe throttled mac
MAC(s) throttled
MAC                Ingress Port
00c1.00aa.006c           ATM1/0/0.101
007c.009e.0070           ATM1/0/0.101
0097.009d.007a           ATM1/0/0.101
008c.0077.0082           ATM1/0/0.101
00b5.00a8.009f           ATM1/0/0.101
00a4.0088.00b5           ATM1/0/0.101
```

The table below describes the significant fields shown in the display.

Table 26: show pppoe throttled mac Field Descriptions

Field	Description
MAC	MAC address whose PPPoE session requests are limited.
Ingress Port	Interface port to which the MAC address attempted to set up a connection.

Related Commands

Command	Description
sessions throttle	Configures PPPoE connection throttling in BBA-group configuration mode.

show sss circuits

Note Effective with Cisco IOS Release 15.0(1)S, the show sss circuits command is replaced by the **show subscriber circuits** command. See the **show subscriber circuits** command for more information.

To display Subscriber Service Switch (SSS) circuits information, use the **show sss circuits** command in privileged EXEC mode.

show sss circuits

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.0(1)S	This command was replaced by the **show subscriber circuits** command.

Usage Guidelines

You can use the **show sss circuits** command to display detailed information about the subscriber switch circuits on the router. This command also displays encapsulation information that can be used for debugging.

Examples

The following is sample output from the **show sss circuits** command:

```
Router# show sss circuits
Current Subscriber Circuit Information: Total number of circuits 1
Common Circuit ID 0             Serial Num 2          Switch ID 1671285332
---------------------------------------------------------------------------
   Status  Encapsulation
   UP flg  len dump
   Y  AES  18  00605C47 AF880060 2FBB3E88 8100000A 0800
   Y  AES  0
```

The table below describes the significant fields shown in the display.

Table 27: show sss circuits Field Descriptions

Field	Description
Total number of circuits	Total number of SSS circuits.
Common Circuit ID	Common circuit ID for two or more SSS circuits.
Serial Num	Serial number of the SSS circuit.
Switch ID	SSS ID.
Status	Status of the flag.
Encapsulation	Type of the encapsulation used or configured.
AES	The Advanced Encryption Standard (AES).

Related Commands

Command	Description
show sss session	Displays SSS session status.

show sss session

Note Effective with Cisco IOS Release 15.0(1)S, the **show sss session** command is replaced by the **show subscriber session** command. See the **show subscriber session** command for more information.

To display Subscriber Service Switch (SSS) session status, use the **show sss session** command in privileged EXEC mode.

show sss session [all]

Syntax Description

all	(Optional) Provides an extensive report about the SSS sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.0(1)S	This command was replaced by the **show subscriber session** command.

Usage Guidelines

Use this command to verify the correct operation of PPP connections in the SSS environment.

The **show sss session** command reports only the current active SSS sessions. For example, an interface that is configured as an IP subscriber interface has an Intelligent Services Gateway (ISG) session running all the time. If the session cannot become active due to AAA failure(s), it is not listed in the report.

Examples

The following sample output from the **show sss session** command provides a basic report of SSS session activity:

```
Router# show sss session
Current SSS Information: Total sessions 9
Uniq ID Type       State         Service      Identifier                        Last Chg
9       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
10      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
11      PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:01:52
3       PPPoE/PPP  connected     VPDN         user3@cisco.com          2d21h
6       PPPoE/PPP  connected     Local Term   user1                    00:03:35
7       PPPoE/PPP  connected     Local Term   user2                    00:03:35
8       PPPoE/PPP  connected     VPDN         nobody3@cisco.com        00:02:36
```

```
2       PPP        connected     Local Term   user5                   00:05:06
4       PPP        connected     VPDN         nobody2@cisco.com       00:06:52
```

The following sample output from the **show sss session all**command provides a more extensive report of SSS session activity:

```
Router# show sss session
 all
Current SSS Information: Total sessions 9
SSS session handle is 40000013, state is connected, service is VPDN
Unique ID is 9
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:49
Root SIP Handle is DF000010, PID is 49
AAA unique ID is 10
Current SIP options are Req Fwding/Req Fwded
SSS session handle is B0000017, state is connected, service is VPDN
Unique ID is 10
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:05
Root SIP Handle is B9000015, PID is 49
AAA unique ID is 11
Current SIP options are Req Fwding/Req Fwded
SSS session handle is D6000019, state is connected, service is VPDN
Unique ID is 11
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:13
Root SIP Handle is D0000016, PID is 49
AAA unique ID is 12
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 8C000003, state is connected, service is VPDN
Unique ID is 3
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user3@cisco.com
Last Changed 2d21h
Root SIP Handle is D3000002, PID is 49
AAA unique ID is 3
Current SIP options are Req Fwding/Req Fwded
SSS session handle is BE00000B, state is connected, service is Local Term
Unique ID is 6
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user1
Last Changed 00:03:56
Root SIP Handle is A9000009, PID is 49
AAA unique ID is 7
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DC00000D, state is connected, service is Local Term
Unique ID is 7
SIP subscriber access type(s) are PPPoE/PPP
Identifier is user2
Last Changed 00:03:57
Root SIP Handle is 2C00000A, PID is 49
AAA unique ID is 8
Current SIP options are Req Fwding/Req Fwded
SSS session handle is DB000011, state is connected, service is VPDN
Unique ID is 8
SIP subscriber access type(s) are PPPoE/PPP
Identifier is nobody3@cisco.com
Last Changed 00:02:58
Root SIP Handle is 1000000F, PID is 49
AAA unique ID is 9
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 3F000007, state is connected, service is Local Term
Unique ID is 2
SIP subscriber access type(s) are PPP
Identifier is user5
Last Changed 00:05:30
Root SIP Handle is 8A000009, PID is 92
AAA unique ID is 1
```

```
Current SIP options are Req Fwding/Req Fwded
SSS session handle is 97000005, state is connected, service is VPDN
Unique ID is 4
SIP subscriber access type(s) are PPP
Identifier is nobody2@cisco.com
Last Changed 00:07:16
Root SIP Handle is 32000000, PID is 92
AAA unique ID is 5
Current SIP options are Req Fwding/Req Fwded
```

Most of the fields displayed by the **show sss session** and **show sss session all**commands are self-explanatory. The table below describes the significant fields shown in the displays. Any data not described in the table below is used for internal debugging purposes.

Table 28: show sss session Field Descriptions

Field	Description
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
Type	Access protocols relevant to this session.
State	Status of the connection, which can be one of the following states: • connected--The session has been established. • wait-for-req--Waiting for request. • wait-for-auth--Waiting for authorization. • wait-for-fwd--Waiting to be forwarded; for example, waiting for virtual private dialup network (VPDN) service.
Service	Type of service given to the user.
Identifier	A string identifying the user. This identifier may either be the username, or the name used to authorize the session. When **show sss session**command is used on the LNS, this identifier is optional and may not display the username, or the name used to authorize the session on LNS.
Last Chg	Time interval in hh:mm:ss format since the service for this session was last changed.

Related Commands

Command	Description
show vpdn session	Displays session information about the L2TP and L2F protocols, and PPPoE tunnels in a VPDN.

show vpdn session

To display session information about active Layer 2 sessions for a virtual private dialup network (VPDN), use the **show vpdn session** command in privileged EXEC mode.

show vpdn session [**l2f**| **l2tp**| **pptp**] [**all**| **packets [ipv6]**| **sequence**| **state** [*filter*]]

Syntax Description

l2f	(Optional) Displays information about Layer 2 Forwarding (L2F) calls only.
l2tp	(Optional) Displays information about Layer 2 Tunneling Protocol (L2TP) calls only.
pptp	(Optional) Displays information about Point-to-Point Tunnel Protocol (PPTP) calls only.
all	(Optional) Displays extensive reports about active sessions.
packets	(Optional) Displays information about packet and byte counts for sessions.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
sequence	(Optional) Displays sequence information for sessions.
state	(Optional) Displays state information for sessions.
filter	(Optional) One of the filter parameters defined in the table below.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) session information. The **packets** and **all** keywords were added.
12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.

Release	Modification
12.2(13)T	Reports from this command were enhanced with a unique identifier that can be used to correlate a particular session with the session information retrieved from other **show** commands or **debug** command traces.
12.3(2)T	The **l2f**, **l2tp**, and the **pptp** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	The **l2f** keyword was removed.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show vpdn session** command with the **all** and the **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show vpdn session** command to display information about all active sessions using L2TP, L2F, and PPTP.

The output of the **show vpdn session** command displays PPPoE session information as well. PPPoE is supported on ATM permanent virtual connections (PVCs) compliant with RFC 1483 only. PPPoE is not supported on Frame Relay and any other LAN interfaces such as FDDI and Token Ring.

Reports and options for this command depend upon the configuration in which it is used. Use the command-line question mark (?) help function to display options available with the **show vpdn session** command.

The table below defines the filter parameters available to refine the output of the **show vpdn session** command. You can use any one of the filter parameters in place of the *filter* argument.

Table 29: Filter Parameters for the show vpdn session Command

Syntax	Description
interface serial *number*	Filters the output to display only information for sessions associated with the specified serial interface. • *number* --The serial interface number.
interface virtual-template *number*	Filters the output to display only information for sessions associated with the specified virtual template. • *number* --The virtual template number.

Syntax	Description
tunnel id *tunnel-id session-id*	Filters the output to display only information for sessions associated with the specified tunnel ID and session ID. • *tunnel-id* --The local tunnel ID. The range is 1 to 65535. • *session-id* --The local session ID. The range is 1 to 65535.
tunnel remote-name *remote-name local-name*	Filters the output to display only information for sessions associated with the tunnel with the specified names. • *remote-name* --The remote tunnel name. • *local-name* --The local tunnel name.
username *username*	Filters the output to display only information for sessions associated with the specified username. • *username* --The username.

The **show vpdn session** command provides reports on call activity for all active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session
L2TP Session Information Total tunnels 1 sessions 4
LocID RemID TunID Intf          Username             State    Last Chg Uniq ID
4     691   13695 Se0/0         nobody2@cisco.com        est    00:06:00  4
5     692   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  8
6     693   13695 SSS Circuit   nobody1@cisco.com        est    00:01:43  9
3     690   13695 SSS Circuit   nobody3@cisco.com        est    2d21h     3
L2F Session Information Total tunnels 1 sessions 2
 CLID   MID    Username                   Intf           State   Uniq ID
 1      2      nobody@cisco.com              SSS Circuit   open    10
 1      3      nobody@cisco.com              SSS Circuit   open    11
%No active PPTP tunnels
PPPoE Session Information Total tunnels 1 sessions 7
PPPoE Session Information
UID    SID    RemMAC         OIntf          Intf      Session
              LocMAC                        VASt      state
3      1      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
6      2      0030.949b.b4a0 Fa2/0          Vi1.1     CNCT_PTA
              0010.7b90.0840               UP
7      3      0030.949b.b4a0 Fa2/0          Vi1.2     CNCT_PTA
              0010.7b90.0840               UP
8      4      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
9      5      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
10     6      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
11     7      0030.949b.b4a0 Fa2/0          N/A       CNCT_FWDED
              0010.7b90.0840
```

The table below describes the significant fields shown in the **show vpdn session** display.

Table 30: show vpdn session Field Descriptions

Field	Description
LocID	Local identifier.
RemID	Remote identifier.
TunID	Tunnel identifier.
Intf	Interface associated with the session.
Username	User domain name.
State	Status for the individual user in the tunnel; can be one of the following states: • est • opening • open • closing • closed • waiting_for_tunnel The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Time interval (in hh:mm:ss) since the last change occurred.
Uniq ID	The unique identifier used to correlate this particular session with the sessions retrieved from other **show** commands or **debug** command traces.
CLID	Number uniquely identifying the session.
MID	Number uniquely identifying this user in this tunnel.
UID	PPPoE user ID.
SID	PPPoE session ID.
RemMAC	Remote MAC address of the host.
LocMAC	Local MAC address of the router. It is the default MAC address of the router.
OIntf	Outgoing interface.

Field	Description
Intf VASt	Virtual access interface number and state.
Session state	PPPoE session state.

The **show vpdn session packets** command provides reports on call activity for all the currently active sessions. The following output is from a device carrying an active PPPoE session:

```
Router# show vpdn session packets

%No active L2TP tunnels
%No active L2F tunnels

PPPoE Session Information Total tunnels 1 sessions 1
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       202333          202337          2832652         2832716
```

The table below describes the significant fields shown in the **show vpdn session packets** command display.

Table 31: show vpdn session packets Field Descriptions

Field	Description
SID	Session ID for the PPPoE session.
Pkts-In	Number of packets coming into this session.
Pkts-Out	Number of packets going out of this session.
Bytes-In	Number of bytes coming into this session.
Bytes-Out	Number of bytes going out of this session.

The **show vpdn session all** command provides extensive reports on call activity for all the currently active sessions. The following output is from a device carrying active L2TP, L2F, and PPPoE sessions:

```
Router# show vpdn session all
L2TP Session Information Total tunnels 1 sessions 4
Session id 5 is up, tunnel id 13695
Call serial number is 3355500002
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:03:53
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 692, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 8
Session id 6 is up, tunnel id 13695
```

```
Call serial number is 3355500003
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:04:22
    52 Packets sent, 52 received
    2080 Bytes sent, 1316 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface
    Remote session id is 693, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 9
Session id 3 is up, tunnel id 13695
Call serial number is 3355500000
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 2d21h
    48693 Packets sent, 48692 received
    1947720 Bytes sent, 1314568 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody2@cisco.com
    Interface
    Remote session id is 690, remote tunnel id 58582
  UDP checksums are disabled
  SSS switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 3
Session id 4 is up, tunnel id 13695
Call serial number is 3355500001
Remote tunnel name is User03
  Internet address is 10.0.0.63
  Session state is established, time since change 00:08:40
    109 Packets sent, 3 received
    1756 Bytes sent, 54 received
  Last clearing of "show vpdn" counters never
  Session MTU is 1464 bytes
  Session username is nobody@cisco.com
    Interface Se0/0
    Remote session id is 691, remote tunnel id 58582
  UDP checksums are disabled
  IDB switching enabled
  FS cached header information:
    encap size = 36 bytes
    4500001C BDDC0000 FF11E977 0A00003E
    0A00003F 06A506A5 00080000 0202E4D6
    02B30000
  Sequencing is off
  Unique ID is 4
L2F Session Information Total tunnels 1 sessions 2
MID: 2
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
Unique ID: 10
  Last clearing of "show vpdn" counters never
MID: 3
User:  nobody@cisco.com
Interface:
State:  open
Packets out: 53
Bytes out: 2264
Packets in: 51
Bytes in: 1274
```

```
Unique ID: 11

Last clearing of "show vpdn" counters never
%No active PPTP tunnels
PPPoE Session Information Total tunnels 1 sessions 7
PPPoE Session Information
SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
1       48696           48696           681765          1314657
2       71              73              1019            1043
3       71              73              1019            1043
4       61              62              879             1567
5       61              62              879             1567
6       55              55              791             1363
7       55              55              795             1363
```

The significant fields shown in the **show vpdn session all** command display are similar to those defined in the show vpdn session packets Field Descriptions and the show vpdn session Field Descriptions tables above.

Related Commands

Command	Description
show sss session	Displays Subscriber Service Switch session status.
show vpdn	Displays basic information about all active VPDN tunnels.
show vpdn domain	Displays all VPDN domains and DNIS groups configured on the NAS.
show vpdn group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information, and current session information.
show vpdn history failure	Displays the content of the failure history table.
show vpdn multilink	Displays the multilink sessions authorized for all VPDN groups.
show vpdn redirect	Displays statistics for L2TP redirects and forwards.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.

shutdown (PVC range)

To deactivate a permanent virtual circuit (PVC) range, use the **shutdown** command in PVC range configuration mode. To reactivate a PVC range, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

PVC range is active.

Command Modes

PVC range configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

In the following example, a PVC range called "range1" is deactivated:

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  shutdown
```

Related Commands

Command	Description
range pvc	Defines a range of ATM PVCs.
show pppatm summary	Deactivates an individual PVC within a PVC range.

shutdown (PVC-in-range)

To deactivate an individual permanent virtual circuit (PVC) within a PVC range, use the **shutdown** command in PVC-in-range configuration mode. To reactivate an individual PVC within PVC range, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The PVC is active.

Command Modes

PVC-in-range configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

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

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 7/104
   shutdown
```

Related Commands

Command	Description
pvc-in-range	Configures an individual PVC within a PVC range.
shutdown (PVC range)	Deactivates a PVC range.

subscriber access

To configure a network access server (NAS) to enable the Subscriber Service Switch (SSS) to preauthorize the NAS port identifier (NAS-Port-ID) string before authorizing the domain name, or to add the circuit-id key received in the point-to point protocol (PPP) over Ethernet (PPPoE) control message as a unique key to the database, use the **subscriber access**command in global configuration mode. To disable SSS preauthorization, use the **no** form of this command.

subscriber access {**pppoe**| **pppoa**} {**pre-authorize nas-port-id** [**default**| *list-name*] [**send username**]| **unique-key circuit-id** *circuit-id-key*}

no subscriber access {**pppoe**| **pppoa**} **pre-authorize nas-port-id**

Syntax Description

pppoe	Specifies PPPoE.
pppoa	Specifies PPP over ATM (PPPoATM).
pre-authorize nas-port-id	Signals the SSS to preauthorize the NAS-Port-ID string before authorizing the domain name.
default	(Optional) Uses the default method list name instead of the named *list-name*argument.
list-name	(Optional) Authentication, authorization, and accounting (AAA) authorization configured on the Layer 2 Tunnel Protocol (L2TP) Access Concentrator (LAC).
send username	(Optional) Specifies to send the authentication username of the session in the Change_Info attribute (attribute 77).
unique-key	Sets up the unique key for the PPPoE subscriber.
circuit-id *circuit-id-key*	Specifies a unique subscriber circuit-id key.

Command Default

Preauthorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)B	This command was introduced on the Cisco 6400 series, the Cisco 7200 series, and the Cisco 7401 Application Specific Router (ASR).

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the **pppoe**and **pppoa**keywords were added.
12.4(2)T	The **send username** keywords were added.
12.3(14)YM2	This command was integrated into Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7301, Cisco 7204VXR, and Cisco 7206VXR routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The NAS-Port-ID string is used to locate the first service record, which may contain one of three attributes, as follows:

- A restricted set of values for the domain substring of the unauthenticated PPP name.

This filtered service key then locates the final service. See the **vpdn authorize domain**command for more information.

- PPPoE session limit.
- The logical line ID (LLID).

Once NAS port authorization has taken place, normal authorization, which is usually the domain authorization, continues.

Logical Line ID

The LLID is an alphanumeric string of 1 to 253 characters that serves as the logical identification of a subscriber line. The LLID is maintained in a RADIUS server customer profile database and enables users to track their customers on the basis of the physical lines on which customer calls originate. Downloading the LLID is also referred to as "*preauthorization"* because it occurs before normal virtual private dialup network (VPDN) authorization downloads layer L2TP information.

The **subscriber access**command enables LLID and SSS querying only for PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN or Dot1Q) calls; all other calls, such as ISDN, are not supported.

Per-NAS-Port Session Limits for PPPoE

Use the **subscriber access**command to configure the SSS preauthorization on the LAC so that the PPPoE per-NAS-port session limit can be downloaded from the customer profile database. To use PPPoE per-NAS-port session limits, you must also configure the PPPoE Session-Limit per NAS-Port Cisco attribute-value pair in the user profile.

Examples

The following example signals SSS to preauthorize the NAS-Port-ID string before authorizing the domain name. This policy applies only to sessions that have a PPPoE access type.

```
aaa new-model
aaa group server radius sg-llid
```

```
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
 server 172.20.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg-group
aaa authorization network mlist_llid group sg-llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol 12tp
 domain example.com
 initiate-to ip 10.1.1.1
 local name s7200-2
!
vpdn-group 3
 accept dialin
  protocol pppoe
  virtual-template 1
!
! Signals Subscriber Service Switch to preauthorize the NAS-Port-ID string before
! authorizing the domain name.
subscriber access pppoe pre-authorize nas-port-id mlist-llid
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 10.2.2.2 255.255.255.0 secondary
 ip address 10.0.58.111 255.255.255.0
 no cdp enable
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
!
interface ATM4/0.1 point-to-point
 pvc 1/100
  encapsulation aa15snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.20.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.20.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1
```

The following example is identical to the previous example except that it also adds support for sending the PPP authenticating username with the preauthorization in the Connect-Info attribute. This example also includes command-line interface (CLI) suppression on the LLID if the username that is used to authenticate has a domain that includes #184.

```
aaa new-model
aaa group server radius sg-llid
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg-group
 server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization confg-commands
aaa authorization network default group sg-group
aaa authorization network mlist-llid group sg-llid
aaa session-id common
!
username s7200-2 password 0 lab
username s5300 password 0 lab
username sg-group password 0 lab
vpdn enable
!
vpdn-group 2
 request-dialin
 protocol l2tp
 domain example1.com
 domain example1.com#184
 initiate-to ip 10.1.1.1
 local name s7200-2
 l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
 accept dialin
 protocol pppoe
 virtual-template 1
!
subscriber access pppoe pre-authorize nas-port-id mlist-llid send username
!
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression for calls belonging to a VPDN group.
subscriber authorization enable	Enables SSS type authorization.
vpdn authorize domain	Enables domain preauthorization on a NAS.
vpdn l2tp attribute clid mask-method	Configures a NAS to provide L2TP calling line ID suppression globally on the router.

subscriber authorization enable

To enable Subscriber Service Switch type authorization, use the **subscriber authorization enable**command in global configuration mode. To disable the Subscriber Service Switch authorization, use the **no** form of this command.

subscriber authorization enable

no subscriber authorization enable

Syntax Description

This command has no arguments or keywords.

Command Default

Authorization is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This feature was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **subscriber authorization enable** command triggers Subscriber Service Switch type authorization for local termination, even if virtual private dialup network (VPDN) and Stack Group Bidding Protocol (SGBP) are disabled.

Examples

The following example enables Subscriber Service Switch type authorization:

```
subscriber authorization enable
```

Related Commands

Command	Description
subscriber access	Enables Subscriber Service Switch preauthorizationof a NAS port identifier (NAS-Port-ID) string before authorizing the domain name.
vpdn authorize domain	Enables domain preauthorization on a NAS.

subscriber profile

To define a Subscriber Service Switch (SSS) policy for searches of a subscriber profile database, use the **subscriber profile**command in global configuration mode. To change or disable the SSS policy, use the **no** form of this command.

subscriber profile *profile-name*

no subscriber profile *profile-name*

Syntax Description

profile-name	A unique string, which can represent (but is not limited to) keys such as a domain, dialed number identification service (DNIS), port name, or PPP over Ethernet (PPPoE) service name.

Command Default

No default profile name

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This feature was introduced.

Usage Guidelines

This command is used to locally search the subscriber profile database for authorization data when an authentication, authorization, and accounting (AAA) network authorization method list is configured. Make sure that the **aaa authorization network default local** global configuration command is included in the configuration--do *not* use the **aaa authorization network default** command without the **local**keyword.

Examples

The following example provides virtual private dialup network (VPDN) service to users in the domain cisco.com, and uses VPDN group group 1 to obtain VPDN configuration information:

```
!
subscriber profile cisco.com
 service vpdn group 1
```

The following example provides VPDN service to DNIS 1234567, and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile dnis:1234567
 service vpdn group 1
```

The following example provides VPDN service using a remote tunnel (used on the multihop node), and uses VPDN group 1 to obtain VPDN configuration information:

```
!
subscriber profile host:lac
 service vpdn group 1
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
service deny	Denies service for the SSS policy.
service local	Enables local termination service for the SSS policy.
service relay	Enables relay of PAD messages over an L2TP tunnel.
service vpdn group	Provides VPDN service for the SSS policy.

subscriber redundancy

To configure the broadband subscriber session redundancy policy for synchronization between High Availability (HA) active and standby processors, use the **subscriber redundancy** command in global configuration mode. To delete the policy, use the **no** form of this command.

subscriber redundancy {**bulk limit** {**cpu** *percent* **delay** *seconds* [**allow** *sessions*]| **time** *seconds*}| **dynamic limit** {**cpu** *percent* **delay** *seconds*| [**allow** *sessions*]| **periodic-update interval** [*minutes*]}| **delay** *seconds*| **rate** *sessions seconds*| **disable**}

no subscriber redundancy {**bulk limit** {**cpu**| **time**}| **dynamic limit** {**cpu**| **periodic-update interval** [*minutes*]}| **delay**| **rate**| **disable**}

Syntax Description

bulk	Configures a bulk synchronization redundancy policy.
limit	Specifies the synchronization limit.
dynamic	Configures a dynamic synchronization redundancy policy.
cpu *percent*	Specifies, in percent, the CPU busy threshold value. Range: 1 to 100. Default: 90.
delay *seconds*	Specifies the minimum time, in seconds, for a session to be ready before bulk or dynamic synchronization occurs. Range: 1 to 33550.
allow *sessions*	(Optional) Specifies the minimum number of sessions to synchronize when the CPU busy threshold is exceeded and the specified delay is met. Range: 1 to 2147483637. Default: 25.
time *seconds*	Specifies the maximum time, in seconds, for bulk synchronization to finish. Range: 1 to 3000.
periodic-update interval	Enables the periodic update of accounting statistics for subscriber sessions.
minutes	(Optional) Interval, in minutes, for the periodic update. Range: 10 to 1044. Default: 15.
rate *sessions seconds*	Specifies the number of sessions per time period for bulk and dynamic synchronization. • *sessions*—Range: 1 to 32000. Default: 250. • *seconds*—Range: 1 to 33550. Default: 1.

disable	Disables stateful switchover (SSO) for all subscriber sessions.

Command Default

The default subscriber redundancy policy is applied.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Release 3.5S	This command was modified. The **periodic-update interval** keyword and *minutes* argument were added.
15.2(1)S	This command was modified. The **disable** keyword was added.

Usage Guidelines

Cisco IOS HA functionality for broadband protocols and applications allows for SSO and In-Service Software Upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to manage the capability to synchronize subscriber session initiation on the standby processor of a redundant processor system.

- Use the **bulk** keyword to create and modify the redundancy policy used during bulk (startup) synchronization.
- Use the **dynamic** keyword with the **limit** keyword to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and synchronization rates.
- Use the **delay** keyword to establish the minimum session duration for synchronization and to manage dynamic synchronization of short-duration calls.
- Use the **rate** keyword to throttle the number of sessions to be synchronized per period.
- Use the **dynamic** keyword with the **periodic-update interval** keyword to enable subscriber sessions to periodically synchronize their dynamic accounting statistics (counters) on the standby processor. The periodic update applies to new and existing subscriber sessions. All subscriber sessions do not synchronize their data at exactly the same time. Session synchronization is spread out based on the session creation time and other factors. This command is rejected if a previous instance of the command has not finished processing.
- Use the **disable** keyword to disable SSO for all subscriber sessions.

Examples

The following example shows how to configure a 10-second delay when CPU usage exceeds 90 percent during bulk synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy bulk limit cpu 90 delay 10 allow 25
```

The following example shows how to configure a maximum time of 90 seconds for bulk synchronization to be completed:

```
Router(config)# subscriber redundancy bulk limit time 90
```

The following example shows how to configure a 15-second delay when CPU usage exceeds 90 percent during dynamic synchronization, after which 25 sessions will be synchronized before the CCM again checks the CPU usage:

```
Router(config)# subscriber redundancy dynamic limit cpu 90 delay 15 allow 25
```

The following example shows how to configure 2000 sessions to be synchronized per second during bulk and dynamic synchronization:

```
Router(config)# subscriber redundancy rate 2000 1
```

The following example shows how to configure a periodic update so that subscriber sessions synchronize their accounting statistics every 30 minutes:

```
Router(config)# subscriber redundancy dynamic periodic-update interval 30
```

The following example shows how to disable SSO for all subscriber sessions:

```
Router(config)# subscriber redundancy disable
```

Related Commands

Command	Description
show ccm sessions	Displays CCM session information.
show pppatm statistics	Displays PPPoA statistics.
show pppoe statistics	Displays PPPoE statistics.
show ppp subscriber statistics	Displays PPP subscriber statistics.

sw-module heap fp

To fine-tune the Multi-Processor Forwarding (MPF) heap memory allocation required for specific session scaling and application needs, use the **sw-module heap fp**command in global configuration mode. To return the setting to the default (32 MB), use the **no** form of the command.

sw-module heap fp [*megabytes*]

no sw-module heap fp

Syntax Description

megabytes	(Optional) The heap size in megabytes (MB) for the MPF processor. The default size is 32 MB.

Command Default

The default heap memory allocation size is 32 MB.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YM2	This command was introduced in Cisco IOS Release 12.3(14)YM2 and implemented on the Cisco 7200 VXR and Cisco 7301 routers.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

The default heap size is 32 MB if you do not specify otherwise. Once you have changed and saved the MPF heap memory configuration, reboot the router for the MPF memory size adjustment to take effect.

The following table lists the recommended heap memory size by type of deployment and number of sessions configured:

Table 32: Recommended Heap Memory Sizes

Type of Deployment	Number of Sessions	Recommended Heap Size
PTA/LAC/LNS	8000 and over	80 MB

Examples

The following example sets or changes the MPF heap memory size in a router to 80 MB:

```
Router(config)# sw-module heap fp 80
```

Related Commands

Command	Description
clear mpf interface	Clears MPF packet counts on all physical interfaces.
clear mpf punt	Clears MPF per-box punt reason and count.
ip mpf	Enables MPF on the second CPU of a Cisco 7301 or Cisco 7200 VXR router.
show ip cef exact-route	Displays the exact route for a source-destination IP address pair in CEF.
show mpf cpu	Displays the average CPU utilization when MPF is enabled on the second CPU.
show mpf interface	Displays MPF packet count information on each physical interface.
show mpf ip exact-route	Displays the exact route for a source-destination IP address pair in an MPF system.
show mpf punt	Displays the MPF punt reason and punt packet count for the chassis.

tag ppp-max-payload

To establish a range for the PPP maximum payload to be accepted by the Broadband Remote Access Server (BRAS), use the **tag ppp-max-payload** command under a virtual template in BBA group configuration mode. To disable the effect of this command, use the **tag p pp-max-payload deny**command.

tag ppp-max-payload [**minimum** *octets* **maximum** *octets*] **[deny]**

Syntax Description

minimum	(Optional) Specifies a minimum number of octets. The default minimum value is 1492.
maximum	(Optional) Specifies a maximum number of octets. The default maximum value is 1500.
octets	(Optional) The minimum and maximum number (depending on which keyword precedes the value in the command syntax) of octets that can be accepted by the BRAS.
deny	(Optional) Disables the effect of any values previously entered with the **tag ppp-max-payload** command.

Command Default

The physical interface default maximum transmission unit (MTU) value is used.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The value of the ppp-max-payload tag accepted from a client cannot exceed the physical interface MTU minus 8 bytes (PPP over Ethernet [PPPoE] encapsulation plus PPP encapsulation). That is, the maximum accepted value of this tag from any client is limited to the minimum of physical interface MTU minus 8 and the maximum value configured by the **tag ppp-max-payload maximum** *value*.

This maximum value cap set under the BBA group can be critical to network operation because the physical interface default MTU can be extremely high (for example, 4470 octets for an ATM interface) and the BRAS administrator may not want to negotiate such a high maximum receive unit (MRU) for a session. The minimum value limitation is required to protect the BRAS against excessive fragmentation loads due to PPPoE clients negotiating too low a value for the MRU.

Examples

The following example shows the PPP-Max-Payload and IWF PPPoE Tag Support feature 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
 sessions per-mac limit 1
 sessions per-mac iwf limit 2000
 tag ppp-max-payload minimum 1492 maximum 1892
 interface Virtual-Template1
 ppp lcp echo mru verify minimum 1500
```

Related Commands

Command	Description
bba-group pppoe	Enters BBA group configuration mode and defines a PPPoE profile.

test virtual-template subinterface

To determine if a virtual template can support the creation of subinterfaces, use the test virtual-template subinterface command in privileged EXEC mode.

test virtual-template *template* **subinterface**

Syntax Description

template	The identifying string of the virtual template to be tested.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

This command tests the specified virtual template to determine if it can support the creation of virtual access subinterfaces. If the virtual template cannot support subinterfaces, this command lists the commands that are configured on the virtual template and that are incompatible with subinterfaces.

Examples

The following example tests virtual template 1 to determine if it can support subinterfaces. The output shows that the **traffic-shape rate** 50000 8000 8000 1000 command that is configured on virtual template 1 prevents the virtual template from being able to support subinterfaces.

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

Related Commands

Command	Description
debug vtemplate subinterface	Displays debug messages relating to virtual access subinterfaces.
virtual-template subinterface	Enables the creation of virtual access subinterfaces.

vendor-tag circuit-id service

To enable processing of the PPPoE Vendor-Specific tag in a PPPoE Active Discovery Request (PADR) packet, which extracts the Circuit-Id part of the tag and sends it to a AAA server as the NAS-Port-Id attribute in RADIUS access requests, use the **vendor-tag circuit-id service**command in BBA group configuration mode. To disable the command function (default), use the **no** form of this command.

vendor-tag circuit-id service

no vendor-tag circuit-id service

Syntax Description

This command has no argument or keywords.

Command Default

This command is disabled.

Command Modes

BBA group configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

When this command is not enabled and the Broadband Remote Access Server (BRAS) receives a packet with the Vendor-Specific tag attached, the tag is ignored and the session is allowed to come up. The Vendor-Specific tag is extracted and processed for its Circuit-Id part when the **vendor-tag circuit-id service** command is enabled in BBA group configuration mode. Once the command is configured, the BRAS processes incoming PADR packets and sends the Circuit-Id tag to the AAA server as a NAS-Port-Id RADIUS attribute.

Examples

In the following example, outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Session-confirmation (PADS) packets are configured to retain the incoming Vendor-Specific Line-Id tag:

```
bba-group pppoe pppoe-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

Related Commands

Command	Description
vendor-tag circuit-id strip	Removes an incoming Vendor-Specific Line-Id tag from outgoing PADO and PADR packets.

vendor-tag circuit-id strip

Note Effective with Cisco IOS Release 12.2(31)SB2, the **vendor-tag circuit-id strip** command is replaced by the **vendor-tag strip** command. See the **vendor-tag strip** command for more information.

To remove the incoming Vendor-Specific Line-ID tag from outgoing PPPoE Active Discovery Offer and Request (PADO and PADR) packets, use the **vendor-tag circuit-id strip**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

vendor-tag circuit-id strip

no vendor-tag circuit-id strip

Syntax Description

This command has no arguments or keywords.

Command Default

This command's functionality is disabled. In the default condition, outgoing packets from the Broadband Remote Access Server (BRAS) have a digital subscriber line access multiplexer (DSLAM) inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured.

Command Modes

BBA group configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was replaced by the **vendor-tag strip** command.

Usage Guidelines

Outgoing packets from the BRAS will have a digital subscriber line access multiplexer (DSLAM)-inserted Line-ID tag when the **vendor-tag circuit-id service** command is configured. The DSLAM must remove the tag from the PADO packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending out the packets. When the **vendor-tag circuit-id strip** command is configured, the BRAS removes the incoming Vendor-Specific Line-ID tag from the outgoing packets.

Outgoing PADO and PADS packets from the BRAS will have the DSLAM-inserted Circuit-ID tag. The DSLAM must remove the tag from PADO and PADS packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending the packets out, and this is accomplished using the **vendor-tag circuit-id strip** command.

Examples

In the following example, the BRAS removes incoming Vendor-Specific Line-ID tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
 sessions per-mac limit 50
 vendor-tag circuit-id service
 vendor-tag circuit-id strip

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

Related Commands

Command	Description
vendor-tag circuit-id service	Enables processing of the PPPoE Vendor-Specific tag in a PADR packet so the Circuit-ID part can be sent to a AAA server as the NAS-Port-ID attribute in RADIUS access requests.

vendor-tag remote-id service

To enable processing of the PPPoE Vendor-Specific tag in a PPPoE Active Discovery Request (PADR) packet, which extracts the Remote-ID part of the tag and sends it to an AAA server as the NAS-Port-ID attribute in RADIUS access requests, use the **vendor-tag remote-id service**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

vendor-tag remote-id service

no vendor-tag remote-id service

Syntax Description

This command has no argument or keywords.

Command Default

This command's functionality is disabled. In this default condition, when the Broadband Remote Access Server (BRAS) receives a packet with the vendor-specific tag attached, the tag is ignored and the session is allowed to come up.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

When this command is not enabled and the BRAS receives a packet with the Vendor-Specific tag attached, the tag is ignored and the session is allowed to come up. The Vendor-Specific tag is extracted and processed for its Remote-ID part when the **vendor-tag remote-id service** command is enabled in BBA group configuration mode. When the command is configured, the BRAS processes incoming PADR packets and sends the Remote-ID tag to the AAA server as a NAS-Port-ID RADIUS attribute.

Examples

In the following example, outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Session-Confirmation (PADS) packets are configured to retain the incoming Vendor-Specific Line-ID tag:

```
Router(config-bba-group)# bba-group pppoe pppoe-tag
Router(config-bba-group)# sessions per-mac limit 50
Router(config-bba-group)# vendor-tag remote-id service

Router(config-bba-group)# interface FastEthernet0/0.1
Router(config-bba-group)# encapsulation dot1Q 120
Router(config-bba-group)# pppoe enable group pppoe-tag
```

Related Commands

Command	Description
vendor-tag strip	Removes an incoming Vendor-Specific Line-ID tag from outgoing PADO and PADR packets.

vendor-tag strip

To remove the incoming Vendor-Specific Line-ID tag from outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Request (PADR) packets, use the **vendor-tag strip**command in BBA group configuration mode. To disable the command function, use the **no** form of this command.

vendor-tag strip

no vendor-tag strip

Syntax Description

This command has no arguments or keywords.

Command Default

This command’s functionality is disabled. In the default condition, outgoing packets from the Broadband Remote Access Server (BRAS) have a digital subscriber line access multiplexer (DSLAM)-inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured.

Command Modes

BBA group configuration

Command History

Release	Modification
12.2(31)SB2	This command was introduced. This command replaces the **vendor-tag circuit-id strip** command.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Outgoing packets from the BRAS will have a DSLAM-inserted Remote-ID tag when the **vendor-tag remote-id service** command is configured. The DSLAM must remove the tag from the PPPoE Active Discovery (PAD) outgoing packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending out the packets. When the **vendor-tag strip** command is configured, the BRAS removes the incoming Vendor-Specific Line-ID tag from the outgoing packets.

Outgoing PADO and PPPoE Active Discovery Session-Confirmation (PADS) packets from the BRAS will have the DSLAM-inserted Circuit-ID tag. The DSLAM must remove the tag from PADO and PADS packets. If the DSLAM cannot remove the tag, the BRAS must remove it before sending the packets out, and this is accomplished using the **vendor-tag strip** command.

The **vendor-tag circuit-id strip** command may continue to perform its normal function in prior releases, but it is no longer being updated. Support for the **vendor-tag circuit-id strip**command will cease in a future release.

Examples

In the following example, the BRAS removes incoming Vendor-Specific Remote-ID tags from outgoing PADO and PADS packets:

```
bba-group pppoe pppoe-rm-tag
```

```
 sessions per-mac limit 50
 vendor-tag remote-ID service
 vendor-tag strip

interface FastEthernet0/0.1
 encapsulation dot1Q 120
 pppoe enable group pppoe-tag
```

Related Commands

Command	Description
vendor-tag circuit-id strip	Removes the incoming Vendor-Specific Line-ID tag from outgoing PADO and PADR packets.
vendor-tag remote-id service	Enables processing of the PPPoE Vendor-Specific tag in a PADR packet so the Remote-ID part can be sent to a AAA server as the NAS-Port-ID attribute in RADIUS access requests.

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

number	Number of the virtual template to apply, ranging from 1 to 30.

Command Default

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

virtual-template (BBA group)

To configure a PPPoE profile with a virtual template to be used for cloning virtual access interfaces, use the **virtual-template**command in BBA group configuration mode. To remove the virtual template from a PPPoE profile, use the **no** form of this command.

virtual-template *template-number*

no virtual-template *template-number*

Syntax Description

template-number	Identifying number of the virtual template that will be used to clone virtual-access interfaces.

Command Default

A virtual template is not specified.

Command Modes

BBA group configuration (config-bba-group)#

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI3	This command was integrated into Cisco IOS Release 12.3(7)XI3.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE 2.3.0	This command was integrated. This command is supported on ASR 1000 series.

Usage Guidelines

Each PPPoE profile can clone virtual-access interfaces using only one virtual template. If you enter a second **virtual-template** command in a PPPoE profile, it will replace the first **virtual-template** command.

You can configure different PPPoE profiles to use different virtual templates. You can also configure multiple PPPoE profiles to use the same virtual template.

Examples

The following example shows the configuration of two PPPoE profiles:

```
bba-group pppoe vpn1
 virtual-template 1
 sessions per-vc limit 2
 sessions per-mac limit 1
!
bba-group pppoe vpn2
 virtual-template 2
 sessions per-vc limit 2
 sessions per-mac limit 1
!
```

Related Commands

Command	Description
bba-group pppoe	Creates a PPPoE profile.

virtual-template pre-clone

To specify the number of virtual-access interfaces to be created and cloned from a specific virtual template, use the **virtual-template pre-clone** command in global configuration mode. To disable precloning, use the **no** form of this command.

virtual-template *template-number* **pre-clone** *number*

no virtual-template *template-number* **pre-clone** *number*

Syntax Description

template-number	The number of the virtual template interfaces from which the new virtual-access interfaces are created.
number	The number of virtual-access interfaces to be created.

Command Default

Precloning is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 node route processor.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The number of precloned virtual-access interfaces should be set to the number of expected PPPoA and PPPoE sessions.

The precloned virtual-access interfaces will be attached to the PVC upon receipt of the first PPP packet from the client on the PVC. The virtual-access interface will be detached from the PVC upon termination of the PPP session.

When a PPP session is terminated, the virtual-access interface will remain in the router and will be reused. When precloning is disabled, any virtual-access interfaces that were already precloned but have not yet been used will remain in the router for future use.

Examples

The following example shows how to create 1200 precloned virtual-access interfaces on virtual template 1:

```
virtual-template 1 pre-clone 1200
```

Related Commands

Command	Description
encapsulation (ATM)	Configures the AAL and encapsulation type for an ATM VC, VC class, VC, bundle, or PVC range.
show vtemplate	Displays a list of all configured virtual templates.

virtual-template snmp

To allow virtual access registration with Simple Network Management Protocol (SNMP), use the **virtual-template snmp**command in global configuration mode. To disable virtual access with SNMP, use the **no**form of this command.

virtual-template snmp

no virtual-template snmp

Syntax Description

This command has no arguments or keywords.

Command Default

Virtual access registration is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SB.
12.2(33)SB	The default configuration of this command was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4, as described in the Usage Guidelines.

Usage Guidelines

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command is disabled by default. This default setting enhances scaling and prevents a large number of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

With the **virtual-template snmp** command disabled, a router no longer accepts the **snmp trap link-status**command under a virtual-template interface. Instead, the router displays a configuration error message as shown in the following example:

```
Router(config)# interface
 virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual-template interface is already registered in the interfaces MIB.

Examples

The following example shows how to enable virtual access registration with SNMP:

```
Router> enable
Router# configure terminal
Router(config)# virtual-template snmp
Router(config)#
```

Related Commands

Command	Description
snmp trap link-status	Enables the generation of SNMP link traps.

vlan-id dot1q

To enable IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface, use the **vlan-id dot1q** command in interface configuration mode. To disable 802.1Q encapsulation for a specific VLAN, use the **no** form of this command.

vlan-id dot1q *vlan-id*

no vlan-id dot1q *vlan-id*

Syntax Description

vlan-id	VLAN identifier. Valid values range from 1 to 4095.

Command Default

IEEE 802.1Q VLAN encapsulation is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command allows you to enable IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface without associating the VLAN with a subinterface. Configuring 802.1Q VLANs on the main interface without using up subinterfaces increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

You can configure a VLAN on a main interface and at the same time configure VLANs on subinterfaces of the same interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time. To configure PPPoE over 802.1Q VLAN support on a subinterface, use the **encapsulation dot1q** and **pppoe enable** commands in interface configuration mode.

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

Examples

The following example shows how to configure PPPoE over an 802.1Q VLAN on Fast Ethernet interface 0/0:

```
interface fastethernet 0/0
```

```
 no ip address
 no ip mroute-cache
 duplex half
 vlan-id dot1q 20
  pppoe enable group PPPOE
  exit-vlan-config
```

The following example configures Ethernet interface 0 to bridge packets using VLAN ID 100 and assigns the interface to bridge group 1:

```
interface ethernet 0
 vlan-id dot1q 100
  description bridged vlan 100
  bridge-group 1
 bridge-group 1
```

Related Commands

Command	Description
debug pppoe	Displays debugging information for PPPoE sessions.
pppoe enable	Enables PPPoE sessions on an Ethernet interface or subinterface.
vlan-range dot1q	Enables IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface.
encapsulation dot1q	Enables PPPoE over 802.1Q VLAN support on a subinterface.

vlan-range dot1q

To enable IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface, use the **vlan-range dot1q** command in interface configuration mode. To disable 802.1Q encapsulation for a range of VLANs, use the **no** form of this command.

vlan-range dot1q *start-vlan-id end-vlan-id* **[native]**

no vlan-range dot1q *start-vlan-id end-vlan-id*

Syntax Description

start-vlan-id	VLAN identifier of the first VLAN in the range. Valid values range from 1 to 4095.
end-vlan-id	VLAN identifier of the last VLAN in the range. Valid values range from 1 to 4095.
native	(Optional) Instructs the interface to bridge untagged (native) packets.

Command Default

IEEE 802.1Q VLAN encapsulation is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

This command allows you to enable IEEE 802.1Q VLAN encapsulation for a range of VLANs on an Ethernet interface without associating each VLAN with a subinterface. Configuring an 802.1Q VLAN range on the main interface without using up subinterfaces increases the number of VLANs that can be configured on a router to 4000 VLANs per interface.

You can configure a VLAN range on a main interface and at the same time configure VLANs outside the range on subinterfaces of the same interface. However, you cannot configure a specific VLAN on the main interface and on a subinterface at the same time. To configure PPPoE over 802.1Q VLAN support on a subinterface, use the **encapsulation dot1q** and **pppoe enable** commands in interface configuration mode.

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

To bridge both tagged and untagged packets, regardless of their VLAN ID, you do not need to create a VLAN ID range.

Examples

The following example shows how to configure PPPoE over a range of 802.1Q VLANs on Fast Ethernet interface 0/0:

```
interface fastethernet 0/0
 no ip address
 no ip mroute-cache
 duplex half
 vlan-range dot1q 20 30
  pppoe enable group PPPOE
  exit-vlan-config
```

The following example configures Ethernet interface 0 to bridge untagged (native) packets using a range of VLAN IDs from 1 to 500 and assigns the interface to bridge group 1:

```
interface ethernet 0
 vlan-range dot1q 1 500 native
  description 1 to 500
  bridge-group 1
 bridge-group 1
```

Related Commands

Command	Description
debug pppoe	Displays debugging information for PPPoE sessions.
pppoe enable	Enables PPPoE sessions on an Ethernet interface or subinterface.
vlan-id dot1q	Enables IEEE 802.1Q VLAN encapsulation for a specific VLAN on an Ethernet interface.
encapsulation dot1q	Enables PPPoE over 802.1Q VLAN support on a subinterface.

vpdn authorize domain

To enable domain preauthorization on a network access server (NAS), use the **vpdn authorize domain** command in global configuration mode. To disable domain preauthorization, use the **no** form of this command.

vpdn authorize domain

no vpdn authorize domain

Syntax Description

This command has no arguments or keywords.

Command Default

Domain preauthorization is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A domain preauthorization RADIUS user profile must also be created. See the Examples section and refer to the *Cisco IOS Security Configuration Guide* for information on how to create these profiles.

Examples

Examples

The following example shows the configuration necessary for an L2TP access concentrator (LAC) to participate in domain preauthorization:

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

Examples

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
 check_items= {
 2=cisco
 }
 reply_attributes= {
 9,1="vpdn:vpn-domain-list=net1.com,net2.com"
 6=5
 }
 }
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

vpn service

To configure a static domain name, use the **vpn service** command in ATM VC, ATM VC class or VC class configuration mode or in PVC range configuration mode. To remove a static domain name, use the **no** form of this command.

vpn service *domain-name* **[replace-authen-domain]**

no vpn service *domain-name* **[replace-authen-domain]**

Syntax Description

domain-name	Static domain name.
replace-authen-domain	(Optional) Specifies that when a static name is configured and VPDN preauthentication is configured, the domain name specified for VPN service replaces the domain field in the username for authentication.

Command Default

No default behavior or values

Command Modes

ATM VC configuration ATM VC class configuration PVC range configuration

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)XI7	The **replace-authen-domain** keyword was added and this command was integrated into Cisco IOS Release 12.2(7)XI7.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **vpn service** command in a permanent virtual circuit (PVC), VC class configuration, or PVC range configuration so that PPP over ATM (PPPoA) or PPP over Ethernet over ATM (PPPoEoA) sessions in those PVCs will be forwarded according to the domain name supplied, without starting PPP.

To replace the VPN service domain name with the domain name from the username during preauthentication, use this command with the **replace-authen-domain** keyword, in conjunction with the **vpdn authen-before-forward** command.

Examples

In the following partial example, VPDN group 1 is selected for PPPoA session forwarding based on the domain name example.com:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.com
 initiate-to ip 10.1.1.1 priority 1
.
.
.
interface ATM1/0.1 multipoint
 pvc 101
  encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net
```

In the following partial example using the **replace-authen-domain** keyword, the domain field is replaced by the domain name during preauthentication:

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain example.net
 authen-before-forward
 initiate-to ip 10.1.1.1 priority 1
.
.
.
interface atm 4/0
 ip address 3.0.0.2 255.255.0.0
 pvc 1/20
encapsulation aal5mux ppp virtual-Template 1
  vpn service example.net replace-authen-domain
```

Related Commands

Command	Description
vpdn authen-before-forward	Enables authentication of all dial-in L2TP sessions before the sessions are forwarded to the tunnel server (global preauthentication).