ac name through logging rate-limit

- access-list template, page 3
- ac name, page 5
- atm pppatm link reset, page 7
- atm route-bridged, page 8
- bba-group pppoe, page 12
- call admission limit, page 14
- call admission load, page 16
- class-range, page 18
- clear call admission statistics, page 20
- clear ip http client cookie, page 22
- clear mpf interface, page 23
- clear mpf punt, page 25
- clear ppp subscriber statistics, page 27
- clear pppatm interface atm, page 28
- clear pppatm statistics, page 30
- clear pppoe, page 31
- clear pppoe derived, page 33
- clear pppoe relay context, page 35
- clear pppoe statistics, page 36
- connection request username, page 37
- connection request password, page 38
- control-packets vlan cos, page 39
- controller shdsl, page 41
- cwmp agent, page 43

- cwmp wan, page 44
- cwmp wan default, page 45
- dialer-group, page 46
- dialer-list protocol, page 48
- dsl enable-training-log, page 52
- dsl equipment-type, page 54
- dsl gain-setting rx-offset, page 56
- dsl gain-setting tx-offset, page 58
- dsl linerate, page 60
- dsl lom, page 62
- dsl max-tone-bits, page 63
- dsl noise-margin, page 65
- dsl operating-mode, page 67
- dsl operating-mode (ADSL over ISDN), page 69
- dsl operating-mode gshdsl, page 71
- dsl power-cutback, page 73
- dsl-mode shdsl symmetric annex, page 74
- ip http digest algorithm, page 77
- ip mpf, page 78
- ip tcp adjust-mss, page 80
- logging rate-limit, page 82
- limit pado service-name, page 85

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.