accelerator through cpu-threshold

accelerator

To enter a specific WAAS Express accelerator configuration mode based on the accelerator being configured, use the **accelerator** command in parameter map configuration mode.

accelerator {**cifs-express** | **http-express** | **ssl-express**}

Syntax Description

cifs-express	Enters WAAS CIFS configuration mode and allows the configuration of Common Internet File System (CIFS)-Express accelerator parameters.
http-express	Enters WAAS HTTP configuration mode and allows the configuration of HTTP-Express accelerator parameters.
ssl-express	Enters WAAS SSL configuration mode and allows the configuration of Secure Sockets Layer (SSL)-Express accelerator parameters.

Command Default

WAAS Express accelerator-specific mode is disabled.

Command Modes

Parameter map configuration (config-profile)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

To use the **accelerator** command, enter parameter map configuration mode by using the **parameter-map type waas** command.

The **accelerator cifs-express** command enters WAAS CIFS configuration mode, the **accelerator http-express** command enters WAAS HTTP configuration mode, and the **accelerator ssl-express** command enters WAAS SSL configuration mode.

After entering a WAAS Express accelerator configuration mode, you can enable the respective accelerator by using the **enable** command. If an accelerator is not enabled, accelerator-specific parameters do not come into effect even if they are configured. Configure the accelerator-specific parameters after entering the respective WAAS Express accelerator configuration mode.

Use the **no** form of the **enable** command to disable an accelerator. Use the **exit** command to exit a specific WAAS Express accelerator configuration mode.

Examples

The following example shows how to enter WAAS CIFS configuration mode and enable CIFS-Express accelerator:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator cifs-express
Device(config-waas-cifs)# enable
Device(config-waas-cifs)# exit
```

The following example shows how to enter WAAS HTTP configuration mode and enable HTTP-Express accelerator:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator http-express
Device(config-waas-http)# enable
Device(config-waas-http)# exit
```

The following example shows how to enter WAAS SSL configuration mode and enable SSL-Express accelerator:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator ssl-express
Device(config-waas-ssl)# enable
Device(config-waas-ssl)# exit
```

Related Commands

Command	Description
parameter-map type waas	Configures WAAS Express global parameters.
show waas accelerator	Displays information about WAAS Express accelerators.
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.

access-class (X.25)

To configure an incoming access class on virtual terminals, use the **access-class** (X.25) command in line configuration mode.

access-class *access-list-number* **in**

Syntax Description

access-list-number	An integer that identifies the access list. Range is from 1 to 199.
in	Restricts incoming connections between a particular access server and the addresses in the access list.

Command Default

No incoming access class is defined.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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 access list number is used for both incoming TCP access and incoming packet assembler/disassembler (PAD) access.

In the case of TCP access, the access server uses the IP access list defined with the **access-list** command.

For incoming PAD connections, the same numbered X.29 access list is referenced. If you only want to have access restrictions on one of the protocols, you can create an access list that permits all addresses for the other protocol.

Examples

The following example configures an incoming access class on virtual terminal line 4. For information on the **line vty** command, see the publication *Configuring the Route Processor for the Catalyst 8540 and Using Flash Memory Cards*.

```
line vty 4
 access-class 4 in
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
x29 access-list	Limits access to the access server from certain X.25 hosts.

ads-negative-cache

To configure the alternate data stream negative caching feature of Common Internet File System (CIFS)-Express accelerator, use the **ads-negative-cache** command in WAAS CIFS configuration mode. To disable negative caching, use the **no** form of this command.

ads-negative-cache {**enable** | **timeout** *seconds*}
no ads-negative-cache {**enable** | **timeout** *seconds*}

Syntax Description

enable	Enables negative caching for alternate data streams.
timeout *seconds*	Specifies the timeout value, in seconds, for negative caching entries. The default value is 3. The range is from 1 to 30.

Command Default

Alternate data stream negative caching is enabled, and the default timeout value is 3 seconds.

Command Modes

WAAS CIFS configuration (config-waas-cifs)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

Before you can enable the **ads-negative-cache** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator cifs-express** command in parameter map configuration mode to enter WAAS CIFS configuration mode.

To enable negative caching, use the **ads-negative-cache enable** command before configuring the timeout for negative cache.

Examples

The following example shows how to enable alternate data stream negative caching and configure the cache timeout:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator cifs-express
Device(config-waas-cifs)# enable
Device(config-waas-cifs)# ads-negative-cache enable
Device(config-waas-cifs)# ads-negative-cache timeout 15
```

Related Commands

Command	Description
accelerator	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
parameter-map type waas	Configures WAAS Express global parameters.
show waas accelerator	Displays information about WAAS Express accelerators.

Command	Description
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.

aps group

To allow more than one protect and working interface and Access Circuit Redundancy (ACR) group to be supported on a router, use the **aps group** command in interface configuration or controller configuration mode. To remove a group, use the **no** form of this command.

aps group [**acr**] *group-number*
no aps group [**acr**] *group-number*

Syntax Description

acr	(Optional) Specifies an ACR group.
group-number	Number of the group. The default is 0.

Command Default

No groups exist.

Note

0 is a valid group number.

Command Modes

Interface configuration (config-if)
Controller configuration (config-controller)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.
15.1(1)S	This command was modified. The **acr** keyword was added.

Usage Guidelines

Use the **aps group**command to specify more than one working and protect interface on a router--for example, working channel for group 0 and protect channel for group 1 on one router, and working channel for group 1 and protect channel for group 0 on another router.

The default group number is 0. The **aps group 0** command does not imply that no groups exist.

The **aps group** command must be configured on both the protect and working interfaces.

Use the **acr**keyword to configure an ACR working or protect interface.

Examples

The following example shows how to configure two working/protect interface pairs. Working interface (3/0/0) is configured in group 10 (the protect interface for this working interface is configured on another router), and protect interface (2/0/1) is configured in group 20.

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.6 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 3/0/0
Router(config-if)# aps group 10
Router(config-if)# aps working 1
Router(config-if)# exit
Router(config)# interface pos 2/0/1
Router(config-if)# aps group 20
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

On the second router, protect interface (4/0/0) is configured in group 10, and working interface (5/0/0) is configured in group 20 (the protect interface for this working interface is configured on another router).

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.7 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 4/0/0
Router(config-if)# aps group 10
Router(config-if)# aps protect 1 10.7.7.6
Router(config-if)# exit
Router(config)# interface pos 5/0/0
Router(config-if)# aps group 20
Router(config-if)# aps working 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps interchassis group

To enable Interchassis Stateful Switchover (IC-SSO) for Multilink PPP (MLPPP) sessions with Multirouter Automatic Protection Switching (MR-APS), use the **aps interchassis group** command in controller configuration mode. To disable this functionality, use the **no** form of this command.

aps interchassis group *group-number*
no aps interchassis group

Syntax Description

group-number	Interchassis Redundancy Manager (ICRM) group number.

Command Default

The IC-SSO for MLPPP sessions with MR-APS is disabled.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
15.1(3)S	This command was introduced on Cisco 7600 series routers.

Usage Guidelines

The **aps interchassis group**commandassociates an Automatic Protection Switching (APS) group with an ICRM group number to facilitate MR-APS across two routers, while maintaining stateful MLPPP sessions across the routers and avoiding session renegotiation in case of APS switchover. This command can only be used on routers that have SONET controllers configured on them.

The ICRM group number is configured on the router using the **interchassis group** command.

Examples

The following example shows how to associate an APS group with an ICRM group number:

```
Router# configure terminal
Router(config)# controller sonet
Router(config-controller)# aps interchassis group 100
```

Related Commands

Command	Description
multi-router aps	Enables MR-APS.
interchassis group	Configures an interchassis group.

aps l2vpn-state detach

To set both the working and protect pseudowires active in an APS configuration, use the **aps l2vpn-state detach** command in controller configuration mode. To deactivate, use the **no** form of this command.

aps l2vpn-statedetach
no aps l2vpn-statedetach

Syntax Description

l2vpn-statedetach	Sets the active and protect pseudowires to stay active.

Command Default

This command is not set by default.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS XE Release 3.18.1SP	This command was introduced on the Cisco ASR 900 Series Routers.

Usage Guidelines

Use the **aps l2vpn-state detach** command in the active-active pseudowire redundancy configuration. This command sets both the working and protect pseudowires in an APS configuration to active.

Note The **aps l2vpn-state detach** command takes effect after a controller **shutdown** command, followed by a **no shutown** command is performed. Alternately, the command can be configured when the controller is in shut state.

Examples

Working Controller Configuration

```
controller sonet 0/1/0
aps group 2
aps adm
aps working 1
aps timers 1 3
aps l2vpn-state detach
aps hspw-icrm-grp 1
```

Protect Controller Configuration

```
controller sonet 0/1/0
aps group 2
aps adm
aps unidirectional
aps protect 1 15.15.15.1
aps timers 1 3
aps l2vpn-state detach
aps hspw-icrm-grp 1
```

Related Commands

Command	Description
aps protect	Enables the interface as a protect interface.
aps working	Configures the interface as a working interface.

arp

To enable Address Resolution Protocol (ARP) entries for static routing over the Switched Multimegabit Data Service (SMDS) network, use the following variation of the **arp** command in global configuration mode. To disable this capability, use the **no** form of this command.

arp *ip-address smds-address* **smds**
no arp *ip-address smds-address* **smds**

Syntax Description

ip-address	IP address of the remote router.
smds-address	12-digit SMDS address in the dotted notation *nnnn.nnnn.nnnn* (48 bits long).
smds	Enables ARP for SMDS.

Command Default

Static ARP entries are not created.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

This command requires a 12-digit (48-bit) dotted-format SMDS address. It does not support 15-digit SMDS addresses.

Examples

The following example creates a static ARP entry that maps the IP address 172.20.173.28 to the SMDS address C141.5797.1313 on interface serial 0:

```
interface serial 0
 arp 172.20.173.28 C141.5797.1313 smds
```

Related Commands

Command	Description
smds enable-arp	Enables dynamic ARP. The multicast address for ARP must be set before this command is issued.
smds static-map	Configures a static map between an individual SMDS address and a higher-level protocol address.

async-write

To configure the async write feature of Common Internet File System (CIFS)-Express accelerator, use the **async-write** command in WAAS CIFS configuration mode. To disable the async write feature, use the **no** form of this command.

async-write {**enable** | **quota-threshold** *mb*}
no async-write {**enable** | **quota-threshold** *mb*}

Syntax Description

enable	Enables the async write operation.
quota-threshold *mb*	Specifies the quota threshold, in megabytes (MB), for async write to perform the optimization. The default quote threshold is 20. The threshold range is from 1 to 1024.

Command Default

The async write feature is enabled, and the default quota threshold is 20 MB.

Command Modes

WAAS CIFS configuration (config-waas-cifs)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

Before you can enable the **async-write** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator cifs-express** command in parameter map configuration mode to enter WAAS CIFS configuration mode.

To enable the async write feature, use the **async-write enable** command before configuring the quota threshold.

Examples

The following example shows how to enable async write and configure the quota threshold:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator cifs-express
Device(config-waas-cifs)# enable
Device(config-waas-cifs)# async-write enable
Device(config-waas-cifs)# async-write quota-threshold 1000
```

Related Commands

Command	Description
accelerator	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
parameter-map type waas	Configures WAAS Express global parameters.
show waas accelerator	Displays information about WAAS Express accelerators.

Command	Description
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.

authentication (L2TP)

To enable Challenge Handshake Authentication Protocol (CHAP) style authentication for Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnels, use the **authentication**command in L2TP class configuration mode. To disable L2TPv3 CHAP-style authentication, use the **no** form of this command.

authentication
no authentication

Syntax Description

This command has no arguments or keywords.

Command Default

L2TPv3 CHAP-style authentication is disabled.

Command Modes

L2TP class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

Two methods of control channel authentication are available in Cisco IOS Release 12.0(29)S and later releases. The L2TPv3 Control Message Hashing feature (enabled with the **digest**command) introduces a more robust authentication method than the older CHAP-style method of authentication enabled with the **authentication**command. You may choose to enable both methods of authentication to ensure interoperability with peers that support only one of these methods of authentication, but this configuration will yield control of which authentication method is used to the peer PE router. Enabling both methods of authentication should be considered an interim solution to solve backward-compatibility issues during software upgrades.

The following table shows a compatibility matrix for the different L2TPv3 authentication methods. PE1 is running a Cisco IOS software release that supports the L2TPv3 Control Message Hashing feature, and the different possible authentication configurations for PE1 are shown in the first column. Each remaining column represents PE2 running software with different available authentication options, and the intersections indicate the different compatible configuration options for PE2. If any PE1/PE2 authentication configuration poses ambiguity on which method of authentication will be used, the winning authentication method is indicated in bold. If both the old and new authentication methods are enabled on PE1 and PE2, both types of authentication will occur.

Table 1: Compatibility Matrix for L2TPv3 Authentication Methods

PE1 Authentication Configuration	PE2 Supporting Old Authentication[1]	PE2 Supporting New Authentication[2]	PE2 Supporting Old and New Authentication[3]
None	None	None New integrity check	None New integrity check

PE1 Authentication Configuration	PE2 Supporting Old Authentication[1]	PE2 Supporting New Authentication[2]	PE2 Supporting Old and New Authentication[3]
Old authentication	Old authentication	--	Old authentication **Old authentication** and new authentication **Old authentication** and new integrity check
New authentication	--	New authentication	New authentication Old authentication and **new authentication**
New integrity check	None	None New integrity check	None New integrity check
Old and new authentication	Old authentication	New authentication	Old authentication New authentication **Old and new authentication** **Old authentication** and new integrity check
Old authentication and new integrity check	Old authentication	--	Old authentication **Old authentication** and new authentication **Old authentication** and new integrity check

[1] Any PE software that supports only the old CHAP-like authentication system.

[2] Any PE software that supports only the new message digest authentication and integrity checking authentication system, but does not understand the old CHAP-like authentication system. This type of software may be implemented by other vendors based on the latest L2TPv3 draft.

[3] Any PE software that supports both the old CHAP-like authentication and the new message digest authentication and integrity checking authentication system, such as Cisco IOS 12.0(29)S or later releases.

Examples

The following example enables CHAP-style authentication for L2TPv3 pseudowires configured using the L2TP class configuration named l2tp class1:

```
Router(config)
# l2tp-class l2tp-class1
Router(config-l2tp-class)
# authentication
```

Related Commands

Command	Description
digest	Enables L2TPv3 control channel authentication or integrity checking.
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.
password	Configures the password used by a PE router for CHAP-style L2TPv3 authentication.

authentication key-chain (OTV)

To configure an authentication key chain string for an edge device authentication, use the **authentication key-chain** command in OTV IS-IS instance configuration mode. To return to the default setting, use the **no** form of this command.

authentication key-chain *key-chain-name*
no authentication key-chain *key-chain-name*

Syntax Description

key-chain-name	Authentication key chain. The *key-chain-name* argument is case-sensitive and can be an alphanumeric string of up to 16 characters in length.

Command Default

No authentication key chain is configured.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The **authentication key-chain** command is used to assign a password in the authentication of link-state packet (LSP) protocol data units (PDUs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs). Only one authentication key chain is applied to an IS-IS interface at one time. If you configure a second **authentication key-chain** command, the first is overridden. You can specify authentication for an entire instance of IS-IS instead of at the interface level by using the **authentication key-chain** command.

Examples

The following example shows how to configure an authentication key chain string for edge device authentication:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# authentication key-chain OTVkey
Router(config-otv-isis)# end
```

Related Commands

Command	Description
show otv	Displays information about OTV.
show otv isis	Displays the IS-IS status and configuration.

authentication mode (OTV)

To configure an Overlay Transport Virtualization (OTV) authentication type, use the **authentication mode** command in OTV IS-IS instance configuration mode. To return to the default setting, use the **no** form of this command.

authentication mode {**md5** | **text**}
no authentication mode {**md5** | **text**}

Syntax Description

md5	Specifies the message digest algorithm (MD5) authentication method.
text	Specifies the cleartext authentication method.

Command Default

The authentication type is not configured.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

Use the **authentication mode** command to configure the authentication type for link-state packet (LSP) protocol data units (PDUs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs) on an interface.

Examples

The following example shows how to specify cleartext authentication:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# authentication mode text
Router(config-otv-isis)# end
```

The following example shows to specify MD5 authentication:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# authentication mode md5
Router(config-otv-isis)# end
```

Related Commands

Command	Description
show otv	Displays information about OTV.
show otv isis	Displays the IS-IS status and configuration.

authentication send-only (OTV)

To disable the authentication check on incoming hello protocol data units (PDUs) on an interface and allow only sending of authinfo, use the **authentication send-only** command in OTV IS-IS instance configuration mode. To return to the default setting, use the **no** form of this command.

authentication send-only
no authentication send-only

Syntax Description

This command has no arguments or keywords.

Command Default

The authentication check is enabled on incoming hello PDUs.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The **authentication send-only** command controls authentication checking on incoming link-state packet (LSP) protocol data units (PDUs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Examples

The following example shows how to disable authentication of hello messages between edge devices:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# authentication send-only
Router(config-otv-isis)# end
```

Related Commands

Command	Description
show otv	Displays information about OTV.
show otv isis	Displays the IS-IS status and configuration.

auto-route-target

To enable the automatic generation of a route target, use the **auto-route-target** command in L2 VFI configuration or VFI autodiscovery configuration mode. To remove the automatically generated route targets, use the **no** form of this command.

auto-route-target
no auto-route-target

Syntax Description

This command has no arguments or keywords.

Command Default

A route target is automatically enabled.

Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support . This command was made available in VFI autodiscovery configuration mode.

Usage Guidelines

Use this command with the **l2 vfi autodiscovery** or the **autodiscovery (MPLS)** command, which automatically creates route targets. The **no** form of this command allows you to remove the automatically generated route targets. You cannot enter this command if route targets have not been automatically created yet.

Examples

The following example shows how to generate route targets for Border Gateway Protocol (BGP) autodiscovered pseudowire members with Label Discovery Protocol (LDP) signaling:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# auto-route-target
```

The following example shows how to remove automatically generated route targets in VFI configuration mode:

```
Device(config-vfi)# no auto-route-target
```

Related Commands

Command	Description
autodiscovery (MPLS)	Designates a VFI as having BGP autodiscovered pseudowire members.
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.
route-target (VPLS)	Specifies a route target for a VPLS VFI.

backup active interface

To activate primary and backup lines on specific X.25 interfaces, use the **backup active interface** command in interface configuration mode. To disable active backup behavior on the X.25 interface, use the **no** form of this command.

backup active interface*X.25-interface number*
no backup active interface*X.25-interface number*

Syntax Description

X.25-interface number	X.25 interface type and number, such as serial 1/3.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

The **backup active interface**command is available only on serial interfaces configured for the X.25 protocol. Use this command to activate dual serial lines (a primary and a backup) to maintain the redundancy and monitoring capability available from the SCC0 and SCC1 links on a Lucent 5ESS switch in a telco data communication network (DCN). The DCN provides telco service providers with communications for network management applications.

This configuration requires that both serial interfaces be on the same Cisco router. Once the **backup active interface**command is configured, the router will bring up leads on the backup X.25 interface, but will ignore Set Asynchronous Balanced Mode (SABM) messages from the Lucent 5ESS switch until the primary interface fails.

Examples

The following partial example shows how to configure a primary and backup X.25 interface for dual serial line management of the Lucent 5ESS switch in a DCN:

```
interface serial 1/0
 description SCC0
 backup active interface serial 1/1
 encapsulation x25 dce
 x25 address 66666666
 x25 ltc 8
 x25 ips 256
 x25 ops 256
 clockrate 9600
!
interface serial 1/1
 description SCC1
 encapsulation x25 dce
 x25 address 66666666
 x25 ltc 8
 x25 ips 256
 x25 ops 256
 clockrate 9600
.
.
.
```

Related Commands

Command	Description
debug backup	Monitors the transitions of an interface going down and then back up.
show backup	Displays interface backup status.

backup delay (L2VPN local switching)

To specify how long a backup pseudowire virtual circuit (VC) should wait before resuming operation after the primary pseudowire VC goes down, use the **backup delay** command in interface configuration mode or xconnect configuration mode.

backup delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	Number of seconds that elapse after the primary pseudowire VC goes down before the Cisco IOS software activates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
disable-delay	Number of seconds that elapse after the primary pseudowire VC comes up before the Cisco IOS software deactivates the secondary pseudowire VC. The range is from 0 to 180. The default is 0.
never	Specifies that the secondary pseudowire VC will not fall back to the primary pseudowire VC if the primary pseudowire VC becomes available again unless the secondary pseudowire VC fails.

Command Default

If a failover occurs, the xconnect redundancy algorithm will immediately switch over or fall back to the backup or primary member in the redundancy group.

Command Modes

Interface configuration (config-if)
Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.

Examples

The following example shows a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer. Once a switchover to the secondary VC occurs, there will be no fallback to the primary VC unless the secondary VC fails.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config)# connect frpw1 serial0/1 50 l2transport
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
```

The following example shows an MPLS xconnect with one redundant peer. The switchover will not begin unless the Layer 2 Tunnel Protocol (L2TP) pseudowire has been down for 3 seconds. After a switchover to the secondary VC occurs, there will be no fallback to the primary until the primary VC has been reestablished and is up for 10 seconds.

```
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config)# connect frpw1 serial0/1 50 l2transport
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 3 10
```

Cisco CMTS Routers: Example

The following example sets a 2-second delay before resuming operation after the primary pseudowire VC goes down.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect  10.2.2.2 22 encapsulation mpls
  backup delay 1 2
```

Related Commands

Command	Description
backup peer	Configures a redundant peer for a pseudowire VC.

backup peer

To specify a redundant peer for a pseudowire virtual circuit (VC), use the **backup peer** command in interface configuration mode or xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

backup peer *peer-router-ip-addr vcid* [**pw-class** *pw-class-name*] [**priority** *value*]
no backup peer *peer-router-ip-addr vcid*

Syntax Description

peer-router-ip-addr	IP address of the remote peer.
vcid	32-bit identifier of the VC between the routers at each end of the layer control channel.
pw-class	(Optional) Specifies the pseudowire type. If not specified, the pseudowire type is inherited from the parent xconnect.
pw-class-name	(Optional) Name of the pseudowire you created when you established the pseudowire class.
priority *value*	(Optional) Specifies the priority of the backup pseudowire in instances where multiple backup pseudowires exist. The default is 1. The range is from 1 to 10.

Command Default

No redundant peer is established.

Command Modes

Interface configuration (config-if)
Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.4	This command was modified. The ability to add up to three backup pseudowires was added. The **priority** keyword was added to assign priority to the backup pseudowires.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

In Cisco IOS XE Release 2.3, only one backup pseudowire is supported. In Cisco IOS XE Release 2.4 and later releases, up to three backup pseudowires are supported.

The Cisco IOS Release 12.2(33)SCF supports up to three backup pseudowires for a primary pseudowire. The priority keyword is optional when only one backup pseudowire is configured. This keyword is a required choice when multiple backup pseudowires are configured.

Examples

The following example shows how to configure a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer:

```
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
RoDeviceuter(config)# interface serial0/0
Device(config-if)# xconnect 10.0.0.1 100 pw-class mpls
Device(config-if-xconn)# backup peer 10.0.0.2 200
```

The following example shows how to configure a local-switched connection between ATM and frame relay using Ethernet interworking. The frame relay circuit is backed up by an MPLS pseudowire.

```
Device(config)# pseudowire-class mpls
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# interworking ethernet
Device(config)# connect atm-fr atm1/0 100/100 s2/0 100 interworking ethernet
Device(config-if)# backup peer 10.0.0.2 100 pw-class mpls
```

The following example shows how to configure a pseudowire with two backup pseudowires:

```
interface ATM4/0.1 point-to-point
 pvc 0/100 l2transport
  encapsulation aal5snap
  xconnect 10.1.1.1 100 pw-class mpls
   backup peer 10.1.1.1 101
   backup peer 10.10.1.1 110 priority 2
   backup peer 10.20.1.1 111 priority 9
```

Cisco CMTS Routers: Example

The following example shows how to set a redundant peer for a pseudowire.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect  10.2.2.2 22 encapsulation mpls
    backup peer 10.3.3.3 33
```

Related Commands

Command	Description
backup delay	Specifies how long the backup pseudowire VC should wait before resuming operation after the primary pseudowire VC goes down.

bfe

Note Effective with Cisco IOS Release 12.2, the **bfe** command is not available in Cisco IOS Software.

To allow the router to participate in emergency mode or to end participation in emergency mode when the interface is configured for **x25 bfe-emergency decision** and **x25 bfe-decision ask**, use the **bfe** command in user EXEC mode.

bfe {**enter** | **leave**} *type number*

Syntax Description

enter	Causes the Cisco IOS software to send a special address translation packet that includes an **enter emergency mode** command to the Blacker Front End (BFE) if the emergency mode window is open. If the BFE is already in emergency mode, this command enables the sending of address translation information.
leave	Disables the sending of address translation information from the Cisco IOS software to the BFE when the BFE is in emergency mode.
type	Interface type.
number	Interface number.

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
10.3	This command was introduced.
12.2	This command became unsupported.

Examples

The following example enables an interface to participate in BFE emergency mode:

```
bfe enter serial 0
```

Related Commands

Command	Description
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
x25 bfe-decision	Specifies how a router configured for X.25 BFE emergency decision will participate in emergency mode.
x25 bfe-emergency	Configures the circumstances under which the router participates in emergency mode.

bridge-domain

To enable RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI), use the **bridge-domain**command in Frame Relay DLCI configuration, interface configuration, interface ATM VC configuration, or PVC range configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* [{**access** | **dot1q** [*tag*] | **dot1q-tunnel**}] [**broadcast**] [**ignore-bpdu-pid**] [**pvst-tlv** *CE-vlan*] [**increment**] [**lan-fcs**] [**split-horizon**]
no bridge-domain *vlan-id*

Syntax Description

vlan-id	The number of the VLAN to be used in this bridging configuration. The valid range is from 2 to 4094.
access	(Optional) Enables bridging access mode, in which the bridged connection does not transmit or act upon bridge protocol data unit (BPDU) packets.
dot1q	(Optional) Enables Institute of Electrical and Electronic Engineers (IEEE) 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If this keyword is not specified, the ingress side assumes a CoS value of 0 for quality of service (QoS) purposes.
tag	(Optional--ATM PVCs only) Specifies the 802.1Q value in the range 1 to 4095. You can specify up to 32 **bridge-domain** command entries using **dot1q** *tag* for a single PVC. The highest tag value in a group of **bridge-domain** commands must be greater than the first tag entered (but no more than 32 greater).
dot1q-tunnel	(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs.
broadcast	(Optional) Enables bridging broadcast mode on this PVC. This option is not supported for multipoint bridging. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
ignore-bpdu-pid	(Optional for ATM interfaces only) Ignores BPDU protocol identifiers (PIDs) and treats all BPDU packets as data packets to allow interoperation with ATM customer premises equipment (CPE) devices that do not distinguish BPDU packets from data packets.
pvst-tlv	(Optional) When the router or switch is transmitting, translates Per-VLAN Spanning Tree Plus (PVST+) BPDUs into IEEE BPDUs. When the router or switch is receiving, translates IEEE BPDUs into PVST+ BPDUs.
CE-vlan	Customer-edge VLAN in the Shared Spanning Tree Protocol (SSTP) tag-length-value (TLV) to be inserted in an IEEE BPDU to a PVST+ BPDU conversion.
increment	(PVC range configuration mode only) (Optional) Increments the bridge domain number for each PVC in the range.

lan-fcs	(Optional) Specifies that the VLAN bridging should preserve the Ethernet LAN frame checksum (FCS) of the Ethernet frames across the ATM network. **Note** This option applies only to routers using a FlexWAN module. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Command Default

Bridging is disabled.

Command Modes

Frame Relay DLCI configuration (config-fr-dlci)
Interface configuration (config-if)--Only the **dot1q** and **dot1q-tunnel** keywords are supported in interface configuration mode.
Interface ATM VC configuration (config-if-atm-vc)
PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(13)E	This command was introduced as the **bridge-vlan** command for the 2-port OC-12 ATM WAN Optical Services Modules (OSMs) on Cisco 7600 series routers and Catalyst 6500 series switches.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E.
12.1(14)E1	This command was integrated into Cisco IOS Release 12.1(14)E1. The **dot1q-tunnel** keyword was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **dot1q-tunnel** keyword is not supported in this release.
12.1(19)E	The **split-horizon** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The **dot1q-tunnel** and **split-horizon** keywords are supported in this release.
12.2(17a)SX	Support was added for the **dot1q-tunnel** keyword in Cisco IOS Release 12.2(17a)SX.
12.2(18)SXE	This command was renamed from **bridge-vlan** to **bridge-domain**. The **access**, **broadcast**, **ignore-bpdu-pid**, and **increment** keywords were added.
12.2(18)SXF2	Support for the **lan-fcs** and **broadcast**keywords was removed. The **ignore-bpdu-pid**and **pvst-tlv**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

RFC 1483 bridging on ATM interfaces supports the point-to-point bridging of Layer 2 packet data units (PDUs) over Ethernet networks. RFC 1490 Frame Relay bridging on Packet over SONET (POS) or serial interfaces that are configured for Frame Relay encapsulation provides bridging of Frame Relay packets over Ethernet networks.

The Cisco 7600 router can transmit BPDUs with a PID of either 0x00-0E or 0x00-07. When the router connects to a device that is fully compliant with RFC 1483 Appendix B, in which the IEEE BPDUs are sent and received by the other device using a PID of 0x00-0E, you must not use the **ignore-bpdu-pid**keyword.

If you do not enter the **ignore-bpdu-pid** keyword, the PVC between the devices operates in compliance with RFC 1483 Appendix B. This is referred to as *strict mode* . Entering the **ignore-bpdu-pid** keyword creates *loose mode* . Both modes are described as follows:

- Without the **ignore-bpdu-pid**keyword, in strict mode, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.
- With the **ignore-bpdu-pid**keyword, in loose mode, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for RFC 1483 data.

Cisco-proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether you enter the **ignore-bpdu-pid** keyword.

Use the **ignore-bpdu-pid** keyword when connecting to devices such as ATM digital subscriber line (DSL) modems that send PVST (or 802.1D) BPDUs with a PID of 0x00-07.

The **pvst-tlv** keyword enables BPDU translation when the router interoperates with devices that understand only PVST or IEEE Spanning Tree Protocol. Because the Catalyst 6500 series switch ATM modules support PVST+ only, you must use the **pvst-tlv** keyword when connecting to a Catalyst 5000 family switch that understands only PVST on its ATM modules, or when connecting with other Cisco IOS routers that understand IEEE format only.

When the router or switch is transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.

When the router or switch is receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.

Note The **bridge-domain**and **bre-connect** commands are mutually exclusive. You cannot use both commands on the same PVC for concurrent RFC 1483 and BRE bridging.

To preserve class of service (CoS) information across the ATM network, use the **dot1q** option. This configuration uses IEEE 802.1Q tagging to preserve the VLAN ID and packet headers as they are transported across the ATM network.

To enable service providers to use a single VLAN to support customers that have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Note The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in “raw” bridging access mode, which is similar to access, except that the connection does act on and transmit BPDU packets.

RFC 1483 bridging is supported on AAL5-MUX and AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulated PVCs. RFC-1483 bridged PVCs must terminate on the ATM interface, and the bridged traffic must be forwarded over an Ethernet interface, unless the **split-horizon** option is used, which allows bridging of traffic across bridged PVCs.

Note RFC 1483 bridging is not supported for switched virtual circuits (SVCs). It also cannot be configured for PVCs on the main interface.

In interface configuration mode, only the **dot1q** and **dot1q-tunnel** keyword options are supported.

Examples

The following example shows a PVC being configured for IEEE 802.1Q VLAN bridging using a VLAN ID of 99:

```
Router# configure terminal

Router(config)# interface ATM6/2

Router(config-if)# pvc 2/101

Router(config-if-atm-vc)# bridge-domain 99 dot1q

Router(config-if-atm-vc)# end
```

The following example shows how to enable BPDU translation when a Catalyst 6500 series switch is connected to a device that understands only IEEE BPDUs in an RFC 1483-compliant topology:

```
Router(config-if-atm-vc)# bridge-domain
100 pvst-tlv 150
```

The **ignore-bpdu-pid** keyword is not used because the device operates in an RFC 1483-compliant topology for IEEE BPDUs.

The following example shows how to enable BPDU translation when a Catalyst 5500 ATM module is a device that understands only PVST BPDUs in a non-RFC1483-compliant topology. When a Catalyst 6500 series switch is connected to a Catalyst 5500 ATM module, you must enter both keywords.

```
Router(config-if-atm-vc)# bridge-domain
100 ignore-bpdu-pid pvst-tlv 150
```

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command:

```
Router(config-if-atm-vc)# bridge-domain
100 dot1q-tunnel ignore-bpdu-pid pvst-tlv 150
```

The following example shows a range of PVCs being configured, with the bridge domain number being incremented for each PVC in the range:

```
Router(config)# interface atm 8/0.100

Router(config-if)# range pvc 102/100 102/199
Router(config-if-atm-range)# bridge-domain 102 increment
```

Related Commands

Command	Description
bre-connect	Enables the BRE over a PVC or SVC.

Command	Description
show atm pvc	Displays the configuration of a particular PVC.

bridge-domain (service instance)

To bind a service instance or a MAC tunnel to a bridge domain instance, use the **bridge-domain** command in either service instance configuration mode or MAC-in-MAC tunnel configuration mode. To unbind a service instance or MAC tunnel from a bridge domain instance, use the**no** form of this command.

bridge-domain *bridge-id* [**split-horizon** [**group** *group-id*]]
no bridge-domain *bridge-id* [**split-horizon** [**group** *group-id*]]

Syntax on the Cisco ASR 1000 Series Aggregation Device
bridge-domain bridge-id [**split-horizon group** *group-id*]
no bridge-domain *bridge-id* [**split-horizon group** *group-id*]

Syntax Description

bridge-id	Numerical identifier for the bridge domain instance. The range is an integer from 1 to the platform-specific maximum (or upper) limit. • The upper limit on the Cisco ASR 1000 device is 4096.
split-horizon	(Optional) Configures a port or service instance as a member of a split-horizon group. • This keyword is not supported in MAC-in-MAC tunnel configuration mode.
group	(Optional) Defines the split-horizon group. • This keyword is not supported in MAC-in-MAC tunnel configuration mode.
group-id	(Optional) Identifier for the split-horizon group. Range is 1 to 65533. • This argument is not supported in MAC-in-MAC tunnel configuration mode. • On the Cisco ASR 1000 device, the only values supported are **0** and **1**.

Command Default

Service instances and MAC tunnels are not bound to a bridge domain instance.

Command Modes

Service instance configuration (config-if-svc)

MAC-in-MAC tunnel configuration (config-tunnel-minm)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SRD	This command was modified. The **split-horizon** keyword was added.
12.2(33)SRE	This command was modified. Support for this command was added in MAC-in-MAC tunnel configuration mode.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use the **bridge-domain**(service instance) command to bind either a service instance or a MAC tunnel to a bridge domain.

Bridge domains cannot be configured under a service instance under a MAC tunnel without encapsulation also being configured.

The Cisco ASR 1000 device does not support MAC tunnels.

Note The **bridge-domain**(config) command allows a user to configure components on a bridge domain. For example, the MAC Address Limiting security component can be configured on a bridge domain using this command.

Examples

The following example shows how to bind a bridge domain to a service instance:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# service instance 100 ethernet
Device(config-if-srv)# encapsulation dot1q 100
Device(config-if-srv)# bridge-domain 200
```

The following example shows how to bind a MAC tunnel to a service instance:

```
Device> enable
Device# configure terminal
Device(config)# ethernet mac-tunnel virtual 100
Device(config-tunnel-minm)# bridge-domain 200
```

Related Commands

Command	Description
bridge-domain (**config**)	Enables a user to configure components on a bridge domain.
ethernet evc	Defines an EVC and enters EVC configuration mode.
ethernet service instance	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
encapsulation dot1ad	Defines the matching criteria to be used in order to map single-tagged 802.1ad frames ingress on an interface to the appropriate service instance. The criteria for this command are single VLAN, range of VLANS, and lists of these two criteria.
encapsulation dot1q	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
encapsulation dot1q second dot1q	Defines the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance.
encapsulation untagged	Defines the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance.

bump (Frame Relay VC-bundle-member)

To configure the bumping rules for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **bump** command in Frame Relay VC-bundle-member configuration mode. To specify that the PVC bundle member does not accept bumped traffic, use the **no**form of this command.

bump {**explicit** *level* | **implicit** | **traffic**}
no bump traffic

Syntax Description

explicit *level*	Specifies the precedence, experimental (EXP), or differentiated services code point (DSCP) level to which traffic on a PVC is bumped when the PVC goes down. For PVC bundles that use precedence or EXP mapping, valid values for the *level* argument are from 0 to 7. For PVC bundles that use DSCP mapping, valid values are from 0 to 63.
implicit	Applies the implicit bumping rule, which is the default, to a single PVC bundle member. The implicit bumping rule is that bumped traffic is to be carried by a PVC that has the lower precedence level.
traffic	Specifies that the PVC accept bumped traffic (the default condition). The **no**form stipulates that the PVC does not accept bumped traffic.

Command Default

The PVC accepts bumped traffic, and implicit bumping is used.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(16)BX	This command was integrated into Cisco IOS Release 12.2(16)BX.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **no bump explicit** and **no bump implicit**commands have no effect.

To change the configured bumping rules for a PVC bundle member, override the current configuration with a new **bump** command entry.

To return to the default condition of implicit bumping, use the **bump implicit** command.

The effects of different bumping configurations are as follows:

- Implicit bumping: If you configure implicit bumping, bumped traffic is sent to the PVC configured to handle the next-lower service level. When the original PVC that bumped the traffic comes back up, it resumes transmission of the configured service level. When the **bump explicit** command is not configured, the **bump implicit**commandtakes effect by default; however, the **bump implicit** command does not appear in the **show running-config** and **show startup-config** command outputs.

- Explicit bumping: If you configure a PVC with the **bump explici t** command, you can specify the service level to which traffic is bumped when that PVC goes down, and the traffic is directed to a PVC mapped with that level. If the PVC that picks up and carries the traffic goes down, the traffic uses the bumping rules for that PVC. You can specify only one service level for bumping.
- Permit bumping: The PVC accepts bumped traffic by default. If the PVC has been previously configured to reject bumped traffic, you must use the **bump traffic** command to return the PVC to its default condition.
- Reject bumping: To configure a discrete PVC to reject bumped traffic when traffic is directed to it, use the **no bump traffic** command.

Note When no alternative PVC can be found to handle bumped traffic, even when there are no packets of that traffic type present, the bundle brings itself down. No messages are displayed unless the **debug frame-relay vc-bundle**command is enabled or the interface-level command **logging event frame-relay vc-bundle status**is enabled. When default (implicit) bumping is used for all PVCs, the PVC that is handling the lowest service level can be configured to bump explicitly to a PVC handling a higher service level.

The following examples show the alerts that appear during configuration. They describe configuration problems that might prevent the bundle from coming up or might cause the bundle to go down unexpectedly:

- The following example shows an alert that appears when the **bump explicit** command is configured:

```
%DLCI 300 could end up bumping traffic to itself
```

It warns that PVC 300 may be configured to bump to a PVC that will in turn bump back to PVC 300, in which case the bundle will go down.

- The following example shows an alert that appears when a PVC that is explicitly bumped to is configured with the **no bump traffic** command:

```
%DLCI 306 is configured for bumping traffic to level 7
```

- The following example shows an alert that appears when the service levels handled by a PVC are changed, which leaves other PVCs explicitly configured to bump to levels that are no longer being handled by that PVC:

```
%DLCI(s) configured for explicitly bumping traffic to DLCI 300
```

- The following example shows an alert that appears when a PVC is configured to explicitly bump to a level that is not yet handled by any PVCs:

```
%Presently no member is configured for level 3
```

- The following example shows an alert that appears when you attempt to explicitly configure bumping to a PVC that is already configured with the **no bump traffic** command:

```
%DLCI configured for level 0 does not accept bumping
```

Examples

The following example configures PVC 101 in the Frame Relay PVC bundle named bundle1 with explicit bumping to the PVC bundle member having a precedence level of 7. PVC 101 is also configured to prohibit traffic from other PVCs from being bumped to it:

```
frame-relay vc-bundle bundle1
 match precedence
 pvc 101
 precedence 5
 no bump traffic
 bump explicit 7
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Specifies the DSCP value or values for a specific Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
protect (Frame Relay VC-bundle-member)	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.
pvc (Frame Relay VC-bundle)	Creates a PVC and PVC bundle member and enters Frame Relay VC-bundle-member configuration mode.

cell-packing

To enable ATM over Multiprotocol Label Switching (MPLS) or Layer 2 Tunneling Protocol Version 3 (L2TPv3) to pack multiple ATM cells into each MPLS or L2TPv3 packet, use the **cell-packing** command in the appropriate configuration mode. To disable cell packing, use the **no** form of this command.

cell-packing *cells* **mcpt-timer** *timer*
no **cell-packing**

Syntax Description

cells	The number of cells to be packed into an MPLS or L2TPv3 packet. The range is from 2 to the maximum transmission unit (MTU) of the interface divided by 52. The default number of ATM cells to be packed is the MTU of the interface divided by 52. If the number of cells packed by the peer provider edge router exceeds this limit, the packet is dropped.
mcpt-timer *timer*	Specifies which timer to use for maximum cell-packing timeout (MCPT). Valid values are 1, 2, or 3. The default value is 1.

Command Default

Cell packing is disabled.

Command Modes

Interface configuration
L2transport PVC configuration--for ATM PVC
L2transport PVP configuration--for ATM PVP
VC class configuration

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.0(29)S	Support for L2TPv3 sessions was added.
12.0(30)S	This command was updated to enable cell packing as part of a virtual circuit (VC) class.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(1)SRE	This command was modified. Support for static pseudowires was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Release	Modification
Cisco IOS XE Release 3.1S.	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **cell-packing** command is available only if you configure the ATM VC or virtual path (VP) with ATM adaptation layer 0 (AAL0) encapsulation. If you specify ATM adaptation layer 5 (AAL5) encapsulation, the command is not valid.

Only cells from the same VC or VP can be packed into one MPLS or L2TPv3 packet. Cells from different connections cannot be concatenated into the same packet.

When you change, enable, or disable the cell-packing attributes, the ATM VC or VP and the MPLS or L2TPv3 emulated VC are reestablished.

If a provider edge (PE) router does not support cell packing, the PE router sends only one cell per MPLS or L2TPv3 packet.

The number of packed cells need not match between the PE routers. The two PE routers agree on the lower of the two values. For example, if PE1 is allowed to pack 10 cells per MPLS or L2TPv3 packet and PE2 is allowed to pack 20 cells per MPLS or L2TPv3 packet, the two PE routers would agree to send no more than 10 cells per packet.

If the number of cells packed by the peer PE router exceeds the limit, the packet is dropped.

If you issue the **cell-packing** command without first specifying the **atm mcpt-timers** command, you get the following error:

```
Please set mcpt values first
```

In order to support cell packing for static pseudowires, both PEs must run Cisco IOS Release 12.2(1)SRE, and the maximum number of cells that can be packed must be set to the same value on each.

Examples

The following example shows cell packing enabled on an interface set up for VP mode. The **cell-packing** command specifies that ten ATM cells be packed into each MPLS packet. The command also specifies that the second maximum cell-packing timeout (MCPT) timer be used.

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 1000 800 500
Router(config-if)# atm pvp 100 l2transport
Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 234 encapsulation mpls
Router(config-if-atm-l2trans-pvp)# cell-packing 10 mcpt-timer 2
```

The following example shows how to configure ATM cell relay over MPLS with cell packing in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm cellpacking
Router(config-vc-class)# encapsulation aal0
Router(config-vc-class)# cell-packing 10 mcpt-timer 1
Router(config-vc-class)# exit
Router(config)# interface atm1/0
Router(config-if)# atm mcpt-timers 100 200 250
Router(config-if)# class-int cellpacking
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over L2TPv3 in VC class configuration mode. The VC class is then applied to an interface.

```
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
!
Router(config)# interface atm1/0
Router(config-if)# class-int aal5class
Router(config-if)# pvc ½00 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation l2tpv3
```

Related Commands

Command	Description
atm mcpt-timers	Creates cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS or L2TPv3 packet.
debug atm cell-packing	Displays ATM cell relay cell packing debugging information.
show atm cell-packing	Displays information about the VCs and VPs that have ATM cell packing enabled.

cipher

To add a cipher suite to a cipher list, use the **cipher** command in cipher list configuration mode. To remove a cipher suite from a cipher list, use the **no** form of this command.

cipher *cipher-suite*
no cipher *cipher-suite*

Syntax Description

cipher-suite	Name of the cipher suite. Valid values include: • dhe-rsa-with-3des-ede-cbc-sha • dhe-rsa-with-aes-128-cbc-sha • dhe-rsa-with-aes-256-cbc-sha • dhe-rsa-with-des-cbc-sha • rsa-with-3des-ede-cbc-sha • rsa-with-aes-128-cbc-sha • rsa-with-aes-256-cbc-sha • rsa-with-des-cbc-sha • rsa-with-rc4-128-md5 • rsa-with-rc4-128-sha

Command Default

A cipher suite does not exist in a cipher list.

Command Modes

Cipher list configuration (config-waas-cipher-list)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

Before you can enable the **cipher** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator ssl-express** command in parameter map configuration mode to enter WAAS SSL configuration mode.

Use the **cipher-list** command in WAAS SSL configuration mode to enter cipher list configuration mode.

Examples

The following example shows how to add a cipher suite to a cipher list:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator ssl-express
Device(config-waas-ssl)# enable
Device(config-waas-ssl)# cipher-list clist
Device(config-waas-cipher-list)# cipher rsa-with-3des-ede-cbc-sha
```

Related Commands

Command	Description
accelerator	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
cipher-list	Creates a cipher list for a WAAS-to-WAAS session.
parameter-map type waas	Configures WAAS Express global parameters.
show waas accelerator	Displays information about WAAS Express accelerators.
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.

cipher-list

To create a cipher list for a Wide-Area Application Services (WAAS)-to-WAAS session, use the **cipher-list** command in WAAS SSL configuration mode. To remove a cipher list, use the **no** form of this command.

cipher-list *list-name*
no cipher-list *list-name*

Syntax Description

list-name	Name of the cipher list.

Command Default

A cipher list does not exist.

Command Modes

WAAS SSL configuration (config-waas-ssl)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Usage Guidelines

A cipher list is customer list of cipher suites that you assign to an SSL connection.

Before you can enable the **cipher-list** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator ssl-express** command in parameter map configuration mode to enter WAAS SSL configuration mode.

Use the **cipher-list** command to create a cipher list and to enter cipher list configuration mode, where you can add a cipher suite to or remove a cipher suite from a cipher list. Use the **cipher** command to add a cipher suite to a cipher list.

Examples

The following example shows how to create a cipher list:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator ssl-express
Device(config-waas-ssl)# enable
Device(config-waas-ssl)# cipher-list clist
```

Related Commands

Command	Description
accelerator	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
cipher	Adds a cipher suite to a cipher list.
parameter-map type waas	Configures WAAS Express global parameters.
services host-service peering	Configures the SSL-Express accelerator host peering service.

Command	Description
show waas accelerator	Displays information about WAAS Express accelerators.
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.
waas-ssl-trustpoint	Associates a trustpoint with SSL-Express accelerator.

class

To associate a map class with a specified data-link connection identifier (DLCI), use the **class** command in Frame Relay DLCI configuration mode or Frame Relay VC-bundle-member configuration mode. To remove the association between the DLCI and the map class, use the **no** form of this command.

class *name*
no class *name*

Syntax Description

name	Name of the map class to associate with the specified DLCI.

Command Default

No map class is defined.

Command Modes

Frame Relay DLCI configuration
Frame Relay VC-bundle-member configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	This command was made available in Frame Relay VC-bundle-member configuration mode.
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.
12.2SX	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.
12.2(33)SCF	This command was integrated into Cisco IOS Release 12.2(33)SCF.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Use this command with DLCIs that were created using the **frame-relay interface-dlci** command and with DLCIs that were created as permanent virtual circuit (PVC) bundle members within a specified Frame Relay PVC bundle. The PVC bundle is created using the **frame-relay vc-bundle** command. The Frame Relay PVC bundle member DLCIs are then created by using the **pvc** command in Frame Relay VC-bundle configuration mode.

A map class applied to the interface is applied to all PVC members in a PVC bundle. A class applied to an individual PVC bundle member supersedes the class applied at the interface level.

The map class is created by using the **map-class frame-relay** command in global configuration mode.

Examples

The following example shows how to define a map class named slow-vcs and apply it to DLCI 100:

```
interface serial 0.1 point-to-point
 frame-relay interface-dlci 100
  class slow-vcs
```

```
map-class frame-relay slow-vcs
 frame-relay cir out 9600
```

The following example shows how to apply a map class to a DLCI for which a **frame-relay map** statement exists. The **frame-relay interface-dlci** command must also be used.

```
interface serial 0.2 point-to-multipoint
 frame-relay map ip 172.16.13.2 100
 frame-relay interface-dlci 100
 class slow-vcs
map-class frame-relay slow_vcs
 frame-relay traffic-rate 56000 128000
 frame-relay idle-timer 30
```

The following example creates a Frame Relay map class named class1 and shows how to assign it to PVC 300 in a Frame Relay PVC bundle named MP-3-static:

```
map-class frame-relay class1
interface serial 1/4
 frame-relay map ip 10.2.2.2 vc-bundle MP-3-static
 frame-relay vc-bundle MP-3-static
 pvc 300
 class HI
```

Example of the class Command for Defining Traffic Classes Inside a 802.1p Domain in Cisco IOS Release 12.2(33)SCF

The following example shows how to define traffic classes for the 8021.p domain with packet CoS values:

```
enable
configure terminal
 policy-map cos7
  class cos2
  set cos 2
  end
```

Example of the class Command for Defining Traffic Classes Inside an MPLS Domain in Cisco IOS Release 12.2(33)SCF

The following example shows how to define traffic classes for the MPLS domain with packet EXP values:

```
enable
configure terminal
 policy-map exp7
  class exp7
  set mpls experimental topmost 2
  end
```

Related Commands

Command	Description
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
map-class frame-relay	Creates a map class for which unique QoS values can be assigned.
pvc (frame-relay vc-bundle)	Creates a PVC and PVC bundle member and enters Frame Relay VC-bundle-member configuration mode.

class (map-list)

To associate a map class with a protocol-and-address combination, use the **class** command in map-list configuration mode.

protocol *protocol-address* **class** *map-class* [**broadcast**] [**trigger**] [**ietf**]

Syntax Description

protocol	S upported protocol, bridging, or logical link control keywords: **appletalk**, **bridging**, **clns**, **decnet**, **dlsw**, **ip**, **ipx**, **llc2**, and **rsrb**.
protocol-address	Protocol address. The **bridge** and **clns** keywords do not use protocol addresses.
map-class	Name of the map class from which to derive quality of service (QoS) information.
broadcast	(Optional) Allows broadcasts on this switched virtual circuit (SVC).
trigger	(Optional) Enables a broadcast packet to trigger an SVC. If an SVC that uses this map class already exists, the SVC will carry the broadcast. This keyword can be configured only if **broadcast** is also configured.
ietf	(Optional) Specifies RFC 1490 encapsulation. The default is Cisco encapsulation.

Command Default

No protocol, protocol address, and map class are defined. If the **ietf** keyword is not specified, the default is Cisco encapsulation. If the **broadcast** keyword is not specified, no broadcasts are sent.

Command Modes

Map-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The **vines** and **xns** arguments were removed because Banyan VINES and Xerox Network Systems are no longer available in the Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

This command is used for Frame Relay SVCs; the parameters within the map class are used to negotiate for network resources. The class is associated with a static map that is configured under a map list.

Examples

In the following example, if IP triggers the call, the SVC is set up with the QoS parameters defined within the class “classip”. However, if AppleTalk triggers the call, the SVC is set up with the QoS parameters defined in the class “classapple”. An SVC triggered by either protocol results in two SVC maps, one for IP and one for AppleTalk.

Two maps are set up because these protocol-and-address combinations are heading for the same destination, as defined by the **dest-addr** keyword and the values following it in the **map-list** command.

```
map-list maplist1 source-addr E164 14085551212 dest-addr E164 15085551212
 ip 131.108.177.100 class classip
 appletalk 1000.2 class classapple
```

In the following example, the **trigger** keyword allows AppleTalk broadcast packets to trigger an SVC:

```
ip 172.21.177.1 class class1 broadcast ietf
appletalk 1000.2 class class1 broadcast trigger ietf
```

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
map-list	Specifies a map group and links it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay SVCs.

class-map type waas

To configure a WAAS Express class map, use the **class-map type waas** command in global configuration mode. To remove a WAAS Express class map, use the **no** form of this command.

class-map type waas [**match-any**] *class-map-name*
no class-map type waas [**match-any**] *class-map-name*

Syntax Description

match-any	Specifies to all statements in the specified class map.
class-map-name	Name of the class map. **Note** The only class-map type supported is **waas_global**.

Command Default

WAAS Express class maps are not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command extends the **class-map**command and enters QoS class-map configuration mode.

Examples

The following example shows how to configure a WAAS Express class map:

```
Router> enable
Router# configure terminal
Router(config)# class-map type waas waas_global
Router(config-cmap)# match tcp any
```

Related Commands

Command	Description
class-map	Defines a class map for matching packets to a specified class.
match tcp	Matches traffic based on the IP address or port options.
parameter-map type waas	Configures WAAS Express global parameters.

clear frame-relay-inarp

To clear dynamically created Frame Relay maps, which are created by the use of Inverse Address Resolution Protocol (ARP), use the **clear frame-relay-inarp** command in privileged EXEC mode.

clear frame-relay-inarp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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.

Examples

The following example clears dynamically created Frame Relay maps:

```
clear frame-relay-inarp
```

Related Commands

Command	Description
frame-relay inverse-arp	Reenables Inverse ARP on a specified interface or subinterface.
show frame-relay map	Displays the current map entries and information about the connections.

clear l2tun

To clear the specified Layer 2 tunnel, use the **clear l2tun** command in privileged EXEC mode.

clear l2tun {**l2tp-class** *l2tp-class-name* | **tunnel id** *tunnel-id* | **local ip** *ip-address* | **remote ip** *ip-address* | **all**}

Syntax Description

l2tp-class *l2tp-class-name*	All tunnels with the specified L2TP class name will be torn down.
tunnel id *tunnel-id*	The tunnel with the specified tunnel ID will be torn down.
local ip *ip-address*	All tunnels with the specified local IP address will be torn down.
remote ip *ip-address*	All tunnels with the specified remote IP address will be torn down.
all	All tunnels will be torn down.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(30)S	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

The following example clears the tunnel with the tunnel ID 65432:

```
Router# clear l2tun tunnel id 65432
```

Related Commands

Command	Description
show l2tun session	Displays the current state of Layer 2 sessions and displays protocol information about an L2TP control channel.
show l2tun tunnel	Displays the current state of a Layer 2 tunnels and displays information about currently configured tunnels, including local and remote L2TP hostnames, aggregate packet counts, and L2TP control channels.

clear l2tun counters

To clear session counters for Layer 2 tunnels, use the **clear l2tun counters**command in privileged EXEC mode.

clear l2tun counters [**session** {**ip-addr** *ip-address* | **tunnel** {**id** *local-id* [*local-session-id*] | **remote-name** *remote-name local-name*} | **username** *username* | **vcid** *vcid*}]

Syntax Description

session	(Optional) Specifies that Layer 2 Tunnel Protocol (L2TP) session counters associated with a particular subset of sessions will be cleared.
ip-addr *ip-address*	(Optional) Specifies that L2TP session counters for sessions associated with a particular peer IP address will be cleared.
tunnel	(Optional) Specifies that L2TP session counters for sessions associated with a particular tunnel will be cleared.
id *local-id* [*local-session-id*]	(Optional) Specifies the tunnel for which L2TP session counters will be cleared using the local tunnel ID, and optionally the local session ID.
remote-name *remote-name local-name*	(Optional) Specifies the tunnel for which L2TP session counters will be cleared using the remote tunnel name and local tunnel name.
username *username*	(Optional) Specifies that L2TP session counters for the sessions associated with a particular username will be cleared.
vcid *vcid*	(Optional) Specifies that L2TP session counters for the sessions associated with a particular virtual circuit ID (VCID) will be cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **clear l2tun counters**command to clear the counters for all sessions. Use the additional syntax options to clear the counters for only the specified subset of sessions.

Examples

The following example clears the session counters for all sessions:

```
Router# clear l2tun counters
```

The following example clears the session counters for only those sessions associated with the peer at IP address 10.1.1.1:

```
Router# clear l2tun counters session ip-addr 10.1.1.1
```

Related Commands

Command	Description
clear l2tun counters tunnel l2tp	Clears global or per-tunnel control message statistics for L2TP tunnels.
show l2tun	Displays general information about Layer 2 tunnels and sessions.
show l2tun counters tunnel l2tp	Displays global or per-tunnel control message statistics for L2TP tunnels, or toggles the recording of per-tunnel statistics for a specific tunnel.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
show l2tun tunnel	Displays the current state of Layer 2 tunnels and information about configured tunnels, including local and remote L2TP hostnames, aggregate packet counts, and control channel information.

clear l2tun counters tunnel l2tp

To clear global or per-tunnel control message statistics for Layer 2 Tunnel Protocol (L2TP) tunnels, use the **clear l2tun counters tunnel l2tp** command in privileged EXEC mode.

clear l2tun counters tunnel l2tp [{**authentication** | **id** *local-id*}]

Syntax Description

authentication	(Optional) Clears the L2TP control channel authentication attribute-value (AV) pair counters.
id *local-id*	(Optional) Clears the per-tunnel control message counters for the L2TP tunnel with the specified local ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **clear l2tun counters tunnel l2tp**command to clear the global L2TP control message counters.

Use the **clear l2tun counters tunnel l2tp id** *local-id*command to clear the per-tunnel L2TP control message counters for the L2TP tunnel with the specified local ID.

Use the **clear l2tun counters tunnel l2tp authentication**command to globally clear only the authentication counters.

Examples

The following example clears the global L2TP control message counters:

```
clear l2tun counters tunnel l2tp
```

The following example clears the per-tunnel L2TP control message counters for the tunnel with the local ID 38360:

```
clear l2tun counters tunnel l2tp id 38360
```

The following example clears the L2TP control channel authentication counters globally:

```
clear l2tun counters tunnel l2tp authentication
```

Related Commands

Command	Description
monitor l2tun counters tunnel l2tp	Enables or disables the collection of per-tunnel control message statistics for L2TP tunnels.
show l2tun counters tunnel l2tp	Displays global or per-tunnel control message statistics for L2TP tunnels.

Command	Description
show l2tun tunnel	Displays the current state of L2TP tunnels and information about configured tunnels.

clear otv arp-nd

To clear all Layer 3-to-Layer 2 address mappings from Address Resolution Protocol (ARP) packets caching information, use the **clear otv arp-nd** command in privileged EXEC mode.

clear otv arp-nd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to clear Layer 3-to-Layer 2 address mappings from the ARP cache:

```
Router> enable
Router# clear otv arp-nd
```

Related Commands

Command	Description
show otv arp-nd-cache	Displays Layer 2 and Layer 3 addresses cached from ARP packet inspection.

clear otv isis

To clear the Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) data, use the **clear otv isis** command in privileged EXEC mode.

clear otv isis [{**overlay** *overlay-interface* | **site**}] *****

Syntax Description

overlay *overlay-interface*	(Optional) Specifies the overlay interface. The range is from 0 to 512.
site	(Optional) Configures the IS-IS Layer 2 site process.
*****	Clears all IS-IS data.

Command Modes

Privileged EXEC (#)…

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to clear all IS-IS data on overlay interface 1:

```
Router# clear otv isis overlay 1 *
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

clear otv isis lspfull

To clear the Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) database, use the **clear otv isis lspfull** command in privileged EXEC mode.

clear otv isis lspfull

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The LSP database becomes full because too many routes are redistributed. Use this command to clear the LSP-full state.

Examples

The following example shows how to clear the LSP database:

```
Router# clear otv isis lspfull
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

clear otv isis neighbors

To clear the counters and resets associated with Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) neighbors, use the **clear otv isis neighbors** command in privileged EXEC mode.

clear otv isis [{**overlay** *overlay-interface* | **site**}] **neighbors**

Syntax Description

overlay *overlay-interface*	(Optional) Specifies the overlay interface. The range is from 0 to 512.
site	(Optional) Configures the IS-IS Layer 2 site process.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to clear the adjacency counters and resets:

```
Router# clear otv isis neighbors
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

clear otv isis rib

To clear the local Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) Routing Information Base (RIB), use the **clear otv isis rib** command in privileged EXEC mode.

clear otv isis rib redistribution [{***** | **mac** | **multicast** {***** | **mapping**}}]

Syntax Description

redistribution	Clears redistribution RIB information.
*****	(Optional) Clears all IS-IS RIB information.
mac	(Optional) Clears MAC address RIB information.
multicast	(Optional) Clears multicast route RIB information.
mapping	(Optional) Clears multicast mapping RIB information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to clear all IS-IS redistribution RIB information:

```
Router# clear otv isis rib redistribution *
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

clear vpdn tunnel pppoe

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

clear vpdn tunnel pppoe

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

Use this command to clear all PPPoE sessions on the device. To clear a specific PPPoE session or set of sessions, use the **clear pppoe** command.

Examples

The following example clears all PPPoE sessions on the device:

```
Router# clear vpdn tunnel pppoe
```

Related Commands

Command	Description
clear pppoe	Clears PPPoE sessions.

clear waas

To clear information about WAAS Express closed connections, statistics, cache, or tokens, use the **clear waas** command in privileged EXEC mode.

clear waas {**cache**{**cifs-express** [**ads-negative-cache**] | **http-express metadatacache** {**all** | **https** | **conditional-response** | **redirect-response** | **unauthorized-response**} | **ssl-express**} | **closed-connections** | **connection** *conn-id* [**forced**] | **token** | **statistics** [{**accelerator** {**cifs-express** | **http-express** | **ssl-express**} | **auto-discovery** [**blacklist**] | **aoim** | **class** | **connection** | **dre** | **errors** | **global** | **lz** | **pass-through** | **peer**}]}

Syntax Description

cache	Clears WAAS Express cache.
cifs-express	Clears Common Internet File System (CIFS)-Express accelerator cache.
ads-negative-cache	(Optional) Clears alternate data stream negative cache.
http-express metadatacache	Clears HTTP metadata cache.
all	Clears all types of metadata caches.
https	Clears HTTPS metadata cache.
conditional-response	Clears conditional-response metadata cache.
redirect-response	Clears redirect-response metadata cache.
unauthorized-response	Clears unauthorized-response metadata cache.
ssl-express	Clears Secure Sockets Layer (SSL)-Express accelerator cache.
closed-connections	Clears information about closed connections.
connection *conn-id*	Clears connection information based on the connection ID.
forced	Clears a specified connection in noninteractive mode.
token	Clears the WAAS Express configuration token used by the WAAS Central Manager (WCM).
statistics	Clears all WAAS Express statistics.
accelerator	Clears accelerator-specific statistics.
cifs-express	Clears CIFS-Express accelerator statistics.
http-express	Clears HTTP-Express accelerator statistics.
ssl-express	Clears SSL-Express accelerator statistics.
auto-discovery [**blacklist**]	Clears autodiscovery and autodiscovery blocked list information for the WAAS Express device.
aoim	Clears statistics for WAAS Express peers and negotiated capabilities.

class	Clears the statistics for each class.
connection	Clears WAAS Express statistics per connection.
dre	Clears Data Redundancy Elimination (DRE) statistics.
errors	Clears WAAS Express error statistics.
global	Clears global WAAS Express statistics.
lz	Clears Lempel-Ziv (LZ) statistics.
pass-through	Clears all pass-through statistics.
peer	Clears peers statistics.

Command Default

Information about closed connections, statistics, or tokens is not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The **cache**, **cifs-express**, **ads-negative-cache**, **http-express metadatacache**, **all**, **https**, **conditional-response**, **redirect-response**, **unauthorized-response** , **ssl-express**, **accelerator**, **http-express**, **connection**, and **errors** keywords were added.

Usage Guidelines

Use this command to clear any information about WAAS Express on the device. The **clear waas connection** *conn-id* command resets the connection and is used to kill connection for some specific reason.

Examples

The following example shows how to clear WAAS Express closed connections information:

```
Device> enable
Device# clear waas closed-connections
```

Related Commands

Command	Description
debug waas	Displays debugging information for different WAAS Express modules.
show waas alarms	Displays WAAS Express status and alarms.
show waas auto-discovery	Displays information about WAAS Express autodiscovery.
show waas connection	Displays information about WAAS Express connections.
show waas statistics aoim	Displays WAAS Express peer information and negotiated capabilities.

Command	Description
show waas statistics application	Displays WAAS Express policy application statistics.
show waas statistics auto-discovery	Displays WAAS Express autodiscovery statistics.
show waas statistics class	Displays statistics for the WAAS Express class map.
show waas statistics dre	Displays WAAS Express DRE statistics.
show waas statistics errors	Displays WAAS Express error statistics.
show waas statistics global	Displays global WAAS Express statistics.
show waas statistics lz	Displays WAAS Express LZ statistics.
show waas statistics pass-through	Displays WAAS Express connections placed in a pass-through mode.
show waas statistics peer	Displays inbound and outbound statistics for peer WAAS Express devices.
show waas status	Displays the status of WAAS Express.
show waas token	Displays the value of the configuration token used by the WAAS Central Manager.
waas cm-register url	Registers a device with the WAAS Central Manager.

clear x25

To restart an X.25 service or Connection-Mode Network Service (CMNS), to clear a switched virtual circuit (SVC), or to reset a permanent virtual circuit (PVC), use the **clear x25** command in privileged EXEC mode.

{**clear x25** {**serial** *number* | {**ethernet** | **fastethernet** | **tokenring** | **fddi**} *number mac-address*} [*vc-number*][*dlci-number*]}

Syntax Description

serial *number*	Local serial interface being used for X.25 service.
{**ethernet** | **fastethernet** | **tokenring** | **fddi**} *number mac-address*	Local CMNS interface (Ethernet, Fast Ethernet, Token Ring, or FDDI interface) and MAC address of the remote device; this information identifies a CMNS service.
vc-number	(Optional) SVC or PVC number, in the range 1 to 4095. If specified, the SVC is cleared or the PVC is reset. If not specified, the X.25 or CMNS service is restarted.
dlci-number	(Optional) When combined with a serial interface number, it triggers a restart event for an Annex G logical X.25 VC.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(3)T	Annex G restart or clear options were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

This command replaces the **clear x25-vc** command, which first appeared in Cisco IOS Release 8.3.

This command is used to disrupt service forcibly on an individual circuit or on all circuits using a specific X.25 service or CMNS service.

If this command is used without the *vc-number* value, a restart event is initiated, which implicitly clears all SVCs and resets all PVCs.

This command allows the option of restarting an Annex G connection per data-link connection identifier (DLCI) number, clearing all X.25 connections, or clearing a specific X.25 logical circuit number on that Annex G link.

Examples

The following example clears the SVC or resets the PVC specified:

```
clear x25 serial 0 1
```

The following example forces an X.25 restart, which implicitly clears all SVCs and resets all PVCs using the interface:

```
clear x25 serial 0
```

The following example restarts the specified CMNS service (if active), which implicitly clears all SVCs using the service:

```
clear x25 ethernet 0 0001.0002.0003
```

The following example clears the specified DLCI Annex G connection (40) from the specified interface:

```
clear x25 serial 1 40
```

Related Commands

Command	Description
clear xot	Clears an XOT SVC or resets an XOT PVC.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
show x25 context	Displays details of an Annex G DLCI link.
show x25 services	Displays information about X.25 services.
show x25 vc	Displays information about active X.25 virtual circuits.

clear xot

To clear an X.25 over TCP (XOT) switched virtual circuit (SVC) or reset an XOT permanent virtual circuit (PVC), use the **clear xot** command in privileged EXEC mode.

clear xot remote *ip-address port* **local** *ip-address port*

Syntax Description

remote *ip-address port*	Remote IP address and port number of an XOT connection ID.
local *ip-address port*	Local IP address and port number of an XOT connection ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

Each SVC or PVC supported by the XOT service uses a TCP connection to communicate X.25 packets. A TCP connection is uniquely identified by the data quartet: remote IP address, remote TCP port, local IP address, and local TCP port. This command form is used to forcibly disrupt service on an individual XOT circuit.

XOT connections are sent to TCP port 1998, so XOT connections originated by the router will have that remote port number, and connections received by the router will have that local port number.

Examples

The following command will clear or reset, respectively, the SVC or PVC using the TCP connection identified:

```
clear xot remote 10.1.1.1 1998 local 172.2.2.2 2000
```

Related Commands

Command	Description
show x25 services	Displays information pertaining to the X.25 services.

clp-bit

To set the ATM cell loss priority (CLP) field in the ATM cell header, use the **clp-bit**command in FRF.5 or FRF.8 connect mode. To disable ATM CLP bit mapping, use the **no** form of this command.

clp-bit {**0** | **1** | **map-de**}
no clp-bit {**0** | **1** | **map-de**}

Syntax Description

0	The CLP field in the ATM cell header is always set to 0.
1	The CLP field in the ATM cell header is always set to 1.
map-de	The discard eligible (DE) field in the Frame Relay header is mapped to the CLP field in the ATM cell header.

Command Default

The default is set to **map-de**.

Command Modes

FRF.5 connect configuration
FRF.8 connect configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

This command maps from Frame Relay to ATM.

Examples

FRF.5: Example

The following example sets the CLP field in the ATM header to 1 for FRF.5:

```
Router(config)# connect network-1 vc-group network-1 ATM3/0 1/35
Router(config-frf5)# clp-bit 1
```

FRF.8: Example

The following example sets the CLP field in the ATM header to 1 for FRF.8:

```
C3640(config)# connect service-1 Serial1/0 16 ATM3/0 1/32 service-interworking
C3640(config-frf8)# clp-bit 1
```

Related Commands

Command	Description
connect (FRF.5)	Connects a Frame Relay DLCI or VC group to an ATM PVC.
de-bit map-clp	Sets the Frame Relay DE bit field in the Frame Relay cell header.

cmns enable

To enable the Connection-Mode Network Service (CMNS) on a nonserial interface, use the **cmns enable** command in interface configuration mode. To disable this capability, use the **no** form of this command.

cmns enable
no cmns enable

Syntax Description

This command has no arguments or keywords.

Command Default

Each nonserial interface must be explicitly configured to use CMNS.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

After this command is processed on the LAN interfaces--Ethernet, Fiber Distributed Data Interface (FDDI), and Token Ring--all the X.25-related interface configuration commands are made available.

Examples

The following example enables CMNS on Ethernet interface 0:

```
interface ethernet 0
 cmns enable
```

Related Commands

Command	Description
x25 route	Creates an entry in the X.25 routing table (to be consulted for forwarding incoming calls and for placing outgoing PAD or protocol translation calls).

collect art

To collect Application Response Time (ART) metrics, use the **collect art** command in Flexible NetFlow flow record configuration mode. To disable the collecting of ART metrics, use the **no** form of this command.

collect art {**all** | **client** {**bytes** | **network time** {**maximum** | **minimum** | **sum**} | **packets**} | **count** {**late responses** | **new connections** | **responses histogram** | **retransmissions** | **transactions**} | **network time** {**maximum** | **minimum** | **sum**} | **response time** {**maximum** | **minimum** | **sum**} | **server** {**bytes** | **packets** | {**network** | **response**} **time** {**maximum** | **minimum** | **sum**}} | **total** {**response** | **transaction**} **time** {**maximum** | **minimum** | **sum**}}
no collect art {**all** | **client** {**bytes** | **network time** {**maximum** | **minimum** | **sum**} | **packets**} | **count** {**late responses** | **new connections** | **responses histogram** | **retransmissions** | **transactions**} | **network time** {**maximum** | **minimum** | **sum**} | **response time** {**maximum** | **minimum** | **sum**} | **server** {**bytes** | **packets** | {**network** | **response**} **time** {**maximum** | **minimum** | **sum**}} | **total** {**response** | **transaction**} **time** {**maximum** | **minimum** | **sum**}}

Syntax Description

all	Collects all ART metrics.
client	Collects ART client metrics.
bytes	Measures the number of bytes sent by a client.
network	Collects ART client network metrics.
time	Collects ART client network time metrics
maximum	Measures the maximum client network time.
minimum	Measures the minimum client network time.
sum	Measures the total client network time.
packets	Measures the number of packets sent by client.
count	Collects ART count metrics.
late	Collects ART count late metrics.
responses	Measures the number of responses.
new	Collects ART count new connection metrics.
connections	Measures the number of new connections.
responses	Measures the number of responses.
histogram	Collects the response count buckets for histogram.
retransmissions	Measures the number of retransmissions.
transactions	Measures the number of transactions.
network	Collects the ART network metrics.

response	Collects the total ART response time metrics.
server	Collects the ART server metrics.
total	Collects the total ART metrics.
transaction	Collects the total ART transaction metrics.

Command Default

No ART metrics are collected.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

Use the **collect art** command to collect the various metrics associated with ART.

The Measurement, Aggregation, and Correlation Engine (MACE) measures TCP and non-TCP traffic. Metrics that are collected by MACE can be categorized as follows:

- Metrics that are provided by the MACE engine, for example, the number of packets and bytes.
- Metrics that are provided by the ART engine, for example, network delay. These metrics are available only for TCP flows.
- Metrics that are provided by Wide Area Application Services (WAAS), for example, Data Redundancy Elimination (DRE) input bytes. These metrics are available only when WAAS is configured and MACE is monitoring the WAAS traffic.

MACE leverages the capabilities of the ART engine to collect measurements associated with TCP-based applications.

Examples

The following example shows how to collect all ART metrics.

```
Router(config)# flow record type mace my-art-record

Router(config-flow-record)# collect art all
```

Related Commands

Command	Description
collect waas	Collects the metrics provided by WAAS.
flow record type mace	Defines the key and nonkey fields that are collected and exported for flow record of type MACE.

collect waas

To collect Wide Area Application Services (WAAS) metrics, use the **collect waas** command in Flexible NetFlow flow record configuration mode. To disable the collecting of WAAS metrics, use the **no** form of this command.

```
collect waas {all | connection mode | {bytes | dre | lz} {input | output}}
no collect waas {all | connection | {bytes | dre | lz} {input | output}}
```

Syntax Description

all	Collects all WAAS metrics.
connection	Configures the WAAS connection.
mode	Configures the connection mode of WAAS.
bytes	Measures input and output bytes of WAAS.
dre	Measures WAAS Data Redundancy Elimination (DRE) metrics.
lz	Measures WAAS Lempel-Ziv (LZ) compression metrics.
input	Measures the number of WAAS input bytes, DRE metrics, or LZ compression metrics.
output	Measures the number of WAAS output bytes, DRE metrics, or LZ compression metrics.

Command Default

No WAAS metrics are collected.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

Use the **collect waas** command to collect the various metrics associated with WAAS.

The Measurement, Aggregation, and Correlation Engine (MACE) measures TCP and non-TCP traffic. WAAS performs operations like compression on the matched packet and stores the statistics in a database. MACE uses a poll mechanism to receive the statistics collected by WAAS each time it needs to prepare the records for exporting.

Note If a flow matches both global WAAS and MACE policies, MACE exports both pre-WAAS and post-WAAS metrics for the flow. If a flow matches the global MACE policy and does not match the global WAAS policy, MACE does not export the post-WAAS metrics.

Once the required measurement metrics are collected, MACE exports the necessary information in an FNF-v9 format to an external NetFlow collector.

Metrics that are collected by MACE can be categorized as follows:

- Metrics that are provided by the MACE engine, for example, the number of packets and bytes, Application ID, Differentiated Services Code Point (DSCP), System Resource Check (SRC), and MACE address.
- Metrics that are provided by the ART engine, for example, network delay. These metrics are available only for TCP flows.
- Metrics that are provided by WAAS, for example, DRE input bytes. These metrics are available only when WAAS is configured and MACE is monitoring the WAAS traffic.

Note All the metrics that are configured as part of the **collect** command are collected and exported to the collector or IP address mentioned in the flow exporter, even if WAAS is not enabled. If WAAS is not enabled, the value of these metrics is zero.

Examples

The following example shows how to collect all WAAS metrics:

```
Router(config)# flow record type mace my-waas-record
Router(config-flow-record)# collect waas all
```

Related Commands

Command	Description
flow record type mace	Configures a flow record for MACE.

connect (Frame Relay)

To define connections between Frame Relay permanent virtual circuits (PVCs), use the **connect** command in global configuration mode. To remove connections, use the **no** form of this command.

connect *connection-name interface dlci* {*I* **interface dlci** | **l2transport**}
no connect *connection-name interface dlci* {**interface dlci** | **l2transport**}

Syntax Description

connection-name	A name for this connection.
interface	Interface on which a PVC connection will be defined.
dlci	Data-link connection identifier (DLCI) number of the PVC that will be connected.
l2transport	Specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(23)S	The l2transport keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

When Frame Relay switching is enabled, the **connect** command creates switched PVCs in Frame Relay networks.

Examples

The following example shows how to define a connection called *frompls1* with DLCI 100 on serial interface 5/0.

```
connect frompls1 Serial5/0 100 l2transport
```

The following example shows how to enable Frame Relay switching and define a connection called *one* between DLCI 16 on serial interface 0 and DLCI 100 on serial interface 1.

```
frame-relay switching
connect one serial0 16 serial1 100
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
mpls l2transport route	Enables routing of Frame Relay packets over a specified VC.

connect (FRF.5)

To configure an FRF.5 one-to-one or many-to-one connection between two Frame Relay end users over an intermediate ATM network, use the **connect** command in global configuration mode. To remove a connection, use the **no** form of this command.

connect *connection-name* {**vc-group** *group-name* | *fr-interface* *fr-dlci*}*atm-interface* *atm-vpi/vci* **network-interworking**
no connect *connection-name* {**vc-group** *group-name* | *fr-interface* *fr-dlci*}*atm-interface* *atm-vpi/vci* **network-interworking**

Syntax Description

connection-name	Connection name. Enter as a string of 15 characters maximum.
vc-group *group-name*	VC group name for a many-to-one FRF.5 connection. Enter as a string of 11 characters maximum. (If the **vc-group keyword**is specified, the interworking type is always network-interworking and does not need to be set as such.)
fr-interface	Frame Relay interface type and number; for example, **serial1/0**.
fr-dlci	Frame Relay data-link connection identifier (DLCI) in the range from 16 to 1007.
atm-interface	ATM interface type and number; for example, **atm1/0**.
atm-vpi / vci	ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0.
network-interworking	FRF.5 network interworking connection. This keyword is not valid if the **vc-group** keyword is specified. (If the **vc-group** keyword is specified, the interworking type is always network-interworking and does not need to be set as such.)

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(8)YN	Enhanced QoS features were added for Cisco 1720, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2610XM-2651XM, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.3(2)T	This feature was integrated into Cisco IOS Release 12.3(2)T for the following platforms: Cisco 1720, Cisco 1721, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2610-2651, Cisco 2610XM-2651XM, Cisco 2691, Cisco 3620, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

Use the **connect** command to connect a group of Frame Relay DLCIs to an ATM permanent virtual circuit (PVC).

To connect to the Frame Relay DLCI that has been configured on the interface, the Frame Relay DLCI must be configured on the interface using the frame-relay interface-dlci switched command.

To disconnect the FRF.5 interworking connection, use the **shutdown** command in FRF.5 connect mode.

Examples

The following example shows how to create an FRF.5 one-to-one connection (not using the **vc-group** keyword):

```
Router(config)#
interface serial0/0
R
outer(config-if)# frame-relay interface-dlci 100 switched
R
outer(config-if)# interface atm1/0
R
outer(config-if)# pvc 0/32
R
outer(config-if-atm-vc)# encapsulation aal5mux frame-relay
Router (config-if-atm-vc)# exit
Router (config-if)# exit
Router(config)#
connect frf5 serial0/0 100 atm1/0 0/32 network-interworking
R
outer(config-frf5)# clp-bit 1
R
outer(config-frf5)# de-bit map-clp
```

The following example shows how to create an FRF.5 many-to-one connection (using the **vc-group** keyword):

```
Router(config)#
interface serial1/0
R
outer(config-if)# frame-relay interface-dlci 100 switched
Router (config-if)# exit
Router(config)#
vc-group friends
Router(config-vc-group)#
serial1/0 16 16
Router(config-vc-group)#
serial1/0 17 17
Router(config-vc-group)#
serial1/0 18 18
Router(config-vc-group)#
serial1/0 19 19
Router (config-vc-group)# exit
Router(config)#
interface atm1/0
R
outer(config-if)# pvc 0/32
R
outer(config-if-atm-vc)# encapsulation aal5mux frame-relay
Router (config-if-atm-vc)# exit
Router (config-if)# exit
Router(config)#
connect frf5-v vc-group friends atm1/0 0/32
```

```
R
outer(config-frf5)# de-bit map-clp
```

Related Commands

Command	Description
clp-bit	Sets the ATM CLP field in the ATM cell header.
de-bit	Sets the Frame Relay DE bit field in the Frame Relay cell header for FRF.5 and FRF.8 service interworking.
encapsulation aal5	Configures the AAL and encapsulation type for an ATM PVC, SVC, VC class, or VC bundle.
frame-relay interface-dlci switched	Indicates that a Frame Relay DLCI is switched.
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, or enters interface-AMT-VC configuration mode.
vc-group	Assigns multiple Frame Relay DLCIs to a VC group.

connect (FRF.8)

To configure an FRF.8 one-to-one mapping between a Frame Relay data-link connection identifier (DLCI) and an ATM permanent virtual circuit (PVC), use the **connect** command in global configuration mode. To remove a connection, use the **no** form of this command.

connect *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI* **service-interworking**
no connect *connection-name FR-interface FR-DLCI ATM-interface ATM-VPI/VCI* **service-interworking**

Syntax Description

connection-name	Specifies a connection name. Enter as a 15-character maximum string.
FR-interface	Specifies the Frame Relay interface type and number, for example, **serial1/0**.
FR-DLCI	Specifies the Frame Relay data-link connection identifier (DLCI) in the range 16 to 1007.
ATM-interface	Specifies the ATM interface type and number, for example **atm1/0**.
ATM-VPI/VCI	Specifies the ATM virtual path identifier/virtual channel identifier (VPI/VCI). If a VPI is not specified, the default VPI is 0.
service-interworking	Specifies FRF.8 service interworking.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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

Use the **connect** command to connect a Frame Relay DLCI to an ATM PVC.

To disconnect the FRF.8 interworking connection, use the **shutdown** connect subcommand.

Examples

The following example shows how to create an FRF.8 connection:

```
router(config)#
interface serial0
router(config-if)# frame-relay interface-dlci 100 switche
d
router(config-if)# interface atm1/0
router(config-if)# pvc 0/32
router(config-if-atm-vc)# encapsulation aal5mux fr-atm-srv
router(config)#
connect service-1 Serial0 100 ATM1/0 0/32 service-interworking
router(config-frf8)# efci-bit map-fecn
```

Related Commands

Command	Description
clp-bit	Sets the ATM CLP field in the ATM cell header.
de-bit map-clp	Sets the EFCI bit field in the ATM cell header.
encapsulation aal5	Configures the AAL and encapsulation type for an ATM PVC, SVC, or VC class.
pvc	Creates an ATM PVC on a main interface or subinterface; enters interface-ATM-VC configuration mode.

connect (L2VPN local switching)

To create Layer 2 data connections between two ports on the same router, use the **connect** command in global configuration mode. To remove such connections, use the **no** form of this command.

Syntax for 12.0S, 12.2S and 12.4T Releases
connect *connection-name type number circuit-id* [{*dlcipvcpvp*}] *type number circuit-id* [{*dlcipvcpvp*}] [{**interworking ip** | **ethernet**}]
no connect *connection-name type number circuit-id* [{*dlcipvcpvp*}] *type number circuit-id* [{*dlcipvcpvp*}] [{**interworking ip** | **ethernet**}]

Syntax for Cisco IOS XE Release 2.5 and Later Releases
connect *connection-name type number type number*
no connect *connection-name type number type number*

Syntax Description

connection-name	A name for this local switching connection.
type	String that identifies the type of interface used to create a local switching connection; for example, serial or Gigabit Ethernet.
number	Integer that identifies the number of the interface; for example, 0/0/0.1 for a Gigabit Ethernet interface.
circuit-id	CEM group ID. This option is used for CEM circuits only.
dlci	(Optional) The data-link connection identifier (DLCI) assigned to the interface.
pvc	(Optional) The permanent virtual circuit (PVC) assigned to the interface, expressed by its vpi/vci (virtual path and virtual channel identifiers).
pvp	(Optional) The permanent virtual path (PVP) assigned to the interface.
interworking ip	(Optional) Specifies that this local connection enables different transport types to be switched locally and causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped. **Note** This keyword is not necessary for configurations that locally switch the same transport type, such as ATM to ATM, or Frame Relay to Frame Relay.
ethernet	(Optional) Specifies that this local connection enables different transport types to be switched locally and causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, leaving a pure Ethernet frame. **Note** This keyword is not necessary for configurations that locally switch the same transport type, such as ATM to ATM, or Frame Relay to Frame Relay.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(27)S	This command was introduced for local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
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 integrated into Cisco IOS XE Release 2.5.
15.1(1)S	This command was modified. The *circuit-id* argument was added.

Examples

The following example shows an Ethernet interface configured for Ethernet, plus an ATM interface configured for AAL5 Subnetwork Access Protocol (SNAP) encapsulation. The **connect** command allows local switching between these two interfaces and specifies the interworking type as IP mode.

```
Router(config)# interface atm 0/0/0
Router(config-if)# pvc 0/100 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5snap
Router(config)# interface fastethernet 6/0/0.1
Router(config-subif)# encapsulation dot1q 100
Router(config)# connect atm-eth-con atm 0/0/0 0/100 fastethernet 6/0/0.1 interworking ip
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.

cpu-threshold

To set the CPU threshold limit, use the **cpu-threshold** command in parameter-map configuration mode. To reset the threshold limit, use the **no** form of this command.

cpu-threshold *maximum-threshold*
no cpu-threshold *maximum-threshold*

Syntax Description

maximum-threshold	The maximum limit. The range is 1 to 100. The default threshold is 80.

Command Default

CPU threshold limit is not set.

Command Modes

Parameter-map configuration (config-profile)

Command History

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

Usage Guidelines

Use this command to set the threshold limit for the CPU device using WAAS Express. WAAS Express accelerates the WAAS optimized flow if the router's CPU utilization exceeds the configured limit.

Examples

The following example shows how to set the CPU threshold:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile)# cpu-threshold 70
```

Related Commands

Command	Description
lz entropy	Enables LZ compression through entropy checking.
parameter-map type waas	Defines a WAAS Express parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery	Configures autodiscovery for WAAS Express.
tfo optimize	Configures compression for WAAS Express.