Cisco IOS Wide-Area Networking Command Reference

March 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco IOS Wide-Area Networking Command Reference

CONTENTS

Introduction

This manual describes the commands used to configure wide-area networking features with Cisco IOS software. For information about configuration, refer to the *Cisco IOS Wide-Area Networking Configuration Guide*.

Some commands required for configuring wide-area networking protocols and broadband access are in other Cisco IOS command references. Use the master list of commands or search online to find these commands.

This manual contains commands for configuring the following technologies and features:

- Frame Relay
- Frame Relay-ATM Interworking
- Layer 2 Tunnel Protocol Version 3 (L2TPv3)
- SMDS
- X.25 and LAPB

This manual is organized alphabetically.

Frame Relay

Frame Relay commands are used to configure access to Frame Relay networks.

For Frame Relay configuration information and examples, refer to the “Configuring Frame Relay” module in the *Cisco IOS Wide-Area Networking Configuration Guide*.

Frame Relay-ATM Interworking

The Frame Relay-ATM interworking commands are used to configure FRF.5 Frame Relay-ATM Network Interworking and FRF.8 Frame Relay-ATM Service Interworking.

For Frame Relay-ATM configuration information and examples, refer to the “Configuring Frame Relay-ATM Interworking” module in the *Cisco IOS Wide-Area Networking Configuration Guide*.

Layer 2 Tunnel Protocol Version 3 (L2TPv3)

L2TPv3 is an Internet Engineering Task Force (IETF) Layer Two Tunneling Protocol Extensions (l2tpext) working group draft that provides several enhancements to L2TP for the capability to tunnel any Layer 2 payload over L2TP. L2TPv3 defines the L2TP protocol for tunneling Layer 2 payloads over an IP core network using Layer 2 virtual private networks (VPNs).

For L2TPv3 configuration information and examples, refer to the "L2TPv3: Layer 2 Tunnel Protocol Version 3" new-feature document for Cisco IOS Release 12.3(2)T.

SMDS

SMDS commands are used to configure Switched Multimegabit Data Service (SMDS), which is a wide-area networking service offered by some regional Bell operating companies (RBOCs) and MCI.

For SMDS configuration information and examples, refer to the "Configuring SMDS" module in the *Cisco IOS Wide-Area Networking Configuration Guide*.

X.25 and LAPB

X.25 and LAPB commands are used to configure the following:

- Link Access Procedure, Balanced (LAPB)
- X.25 services (X.25, X.25 over TCP [XOT] and Connection-Mode Network Service [CMNS])
- Defense Data Network (DDN) X.25
- Blacker Front End (BFE)

For X.25 and LAPB configuration information and examples, refer to the "Configuring X.25 and LAPB" module in the *Cisco IOS Wide-Area Networking Configuration Guide*.

For information on translating between X.25 and another protocol, refer to the "Configuring Protocol Translation and Virtual Asynchronous Devices" module in the *Cisco IOS Terminal Services Configuration Guide*.

Wide-Area Networking Commands

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.

Defaults

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.

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.

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.

Defaults

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.

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.

Table 1 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
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.

auto-route-target

To enable the automatic generation of a route target (RT), use the **auto-route-target** command in L2 VFI configuration mode. To remove the automatically generated RTs, 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

The VPLS Autodiscovery feature automatically generates an RT, so you do not need to enter this command when you configure the feature.

Command Modes

L2 VFI configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

This command works with the **l2 vfi autodiscovery** command, which automatically creates route targets. The **no** version of the 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 removes automatically generated route targets:

```
no auto-route-target
```

Related Commands

Command	Description
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 an RT 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.

Defaults

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.

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
```

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	The 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 1 through 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.

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.

Examples

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

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

The following example shows a local-switched connection between ATM and Frame Relay using Ethernet interworking. The Frame Relay circuit is backed up by an MPLS pseudowire.

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

The following example shows 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
```

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.

Defaults

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.

Defaults

Bridging is disabled.

Command Modes

Frame Relay DLCI configuration
Interface configuration
PVC range configuration

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-subif)# 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.
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 Router

bridge-domain *bridge-id* [**split-horizon group** *group-id*]

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

Syntax Description

bridge-id	Identifier for the bridge domain instance. The range is an integer from 1 to the platform-specific upper limit, where platform-specific upper limit is the maximum allowed by the platform. • Upper limit on the Cisco ASR 1000 router 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 router, the range for the *group-id* argument is 0 to 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.

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 router 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:

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

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

```
Router> enable
Router# configure terminal
Router(config)# ethernet mac-tunnel virtual 100
Router(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.

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.

Defaults

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** command takes 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 explicit** 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	(Optional) 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*	(Optional) Specifies which timer to use. Valid values are 1, 2, or 3. The default value is 1.

Command Default

Cell packing is disabled.

Command Modes

Interface configuration
L2transport VC configuration—for ATM VC
L2transport VP configuration—for ATM VP
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.

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 routers 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
```

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 configures 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 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures 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 1/200 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.

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.

Defaults

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.

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
```

Related Commands

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

Defaults

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 *class-map-name*

no class-map type waas *class-map-name*

Syntax Description

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

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, or tokens, use the **clear waas** command in privileged EXEC mode.

clear waas {**closed-connections** | **connection** *conn-id* [**forced**] | **token** | **statistics** [**auto-discovery** [**blacklist**] | **aoim** | **class** | **dre** | **global** | **lz** | **pass-through** | **peer**]}

Syntax Description

closed-connections	Clears information about closed connections.
conn-id *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.
auto-discovery [**blacklist**]	Clears autodiscovery and autodiscovery blacklist information for the WAAS Express device.
aoim	Clears statistics for WAAS Express peers and negotiated capabilities.
class	Clears the statistics for each class.
dre	Clears Data Redundancy Elimination (DRE) 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.

Usage Guidelines

Use this command to clear any information about WAAS Express on the router. The **clear waas connection conn-id** command resets the connection and is provided to kill a particular connection for some reason.

Examples

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

```
Router> enable
Router# 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.
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.

Defaults

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.

Defaults

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* {*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.

Defaults

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.)

Defaults

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.

Release	Modification
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
Router(config-if)# frame-relay interface-dlci 100 switched
Router(config-if)# interface atm1/0
Router(config-if)# pvc 0/32
Router(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
Router(config-frf5)# clp-bit 1
Router(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
Router(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
Router(config-if)# pvc 0/32
Router(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
Router(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.

Command	Description
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.

Defaults

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 switched
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* [*dlci* | *pvc* | *pvp*] *type number circuit-id* [*dlci* | *pvc* | *pvp*] [**interworking ip** | **ethernet**]

no connect *connection-name type number circuit-id* [*dlci* | *pvc* | *pvp*] *type number circuit-id* [*dlci* | *pvc* | *pvp*] [**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.

de-bit

To set Frame Relay discard-eligible (DE) bit mapping for FRF.5 and FRF.8 network interworking, use the **de-bit command in FRF.5 connect configuration mode or FRF.8 connect configuration mode**. To disable or reset Frame Relay DE bit mapping, use the **no** form of this command.

de-bit {**0** | **1** | **map-clp**}

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

Syntax Description

0	Sets the DE field in the Frame Relay header to 0. This keyword may be used only for FRF.8.
1	Sets the DE field in the Frame Relay header to 1. This keyword may be used only for FRF.8.
map-clp	DE field in the Frame Relay header is set to 1 if one or more cells that belong to a frame have their cell loss priority (CLP) field set. This is the default setting. This keyword may be used for FRF.5 or FRF.8. **Note** **The map-clp** keyword is the only one available for FRF.5.

Defaults

map-clp

Command Modes

FRF.5 connect configuration
FRF.8 connect 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.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T for the following platforms: Cisco 1721, Cisco 2610-2651, Cisco 2610XM-2651XM, Cisco 2691, Cisco 3620, 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

In the default state, the DE bit in the Frame Relay header is set to 1 when one or more ATM cells that belong to a frame have their cell loss priority (CLP) field set to 1 or when the DE field of the Frame Relay service-specific convergence sublayer (FR-SSCS) protocol data unit (PDU) is set to 1.

When the **no de-bit** command and **map-clp** keyword are entered, the FR-SSCS PDU DE field is copied unchanged to the Q.922 core frame DE field, independently of CLP indications received at the ATM layer.

Examples

The following example creates a connection between the virtual circuit (VC) group named “friends” and ATM PVC 0/32 and configures FR DE field mapping to match the ATM CLP field:

```
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)# interface atm3/0
Router(config-if)# pvc 0/32
Router(config-if-atm-vc)# encapsulation aal5mux frame-relay
Router (config-if-atm-vc)# exit
Router (config-if)# exit
Router(config)# connect vc-group friends atm3/0 0/32
Router(config-frf5)# de-bit map-clp
```

Related Commands

Command	Description
clp-bit	Sets the ATM CLP field in the ATM cell header.
connect (FRF.5)	Configures an FRF.5 one-to-one connection or one-to-many connection between two Frame Relay end users over an intermediate ATM network.
connect (FRF.8)	Configures an FRF.8 one-to-one mapping between a Frame Relay DLCI and an ATM PVC.
vc-group	Assigns multiple Frame Relay DLCIs to a VC group.

de-bit map-clp

To set Frame Relay discard eligible (DE) bit mapping for FRF.5 network interworking, use the **de-bit map-clp** command in FRF.5 connect mode. To disable or reset Frame Relay DE bit mapping, use the **no** form of this command.

de-bit map-clp

no de-bit map-clp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

FRF.5 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

In the default state, the DE bit in the Frame Relay header is set to 1 when one or more ATM cells belonging to a frame have their cell loss priority (CLP) field set to 1, or when the DE field of the Frame Relay service specific convergence sublayer (FR-SSCS) protocol data unit (PDU) is set to 1.

When the **no de-bit map-clp** command is entered, the FR-SSCS PDU DE field is copied unchanged to the Q.922 core frame DE field, independent of CLP indications received at the ATM layer.

Examples

The following example creates a connection that connects the virtual circuit (VC) group named friends to ATM PVC 0/32 and configures FR DE field mapping to match the ATM CLP field:

```
Router(config)# vc-group friends
Router(config-vc-group)# serial0 16 16
Router(config-vc-group)# serial0 17 17
Router(config-vc-group)# serial0 18 18
Router(config-vc-group)# serial0 19 19
Router(config)# interface atm3/0
Router(config-if)# pvc 0/32
Router(config-if-atm-vc)# encapsulation aal5mux frame-relay
Router(config)# connect vc-group friends atm3/0 0/32
Router(config-frf5)# de-bit map-clp
```

Related Commands

Command	Description
clp-bit	Sets the ATM CLP field in the ATM cell header.
connect (FRF.5)	Connects a Frame Relay DLCI or VC group to an ATM PVC.
vc-group	Assigns multiple Frame Relay DLCIs to a VC group.

debug l4f

To enable troubleshooting for Layer 4 Forwarding (L4F) flows, use the **debug l4f** command in privileged EXEC mode. To disable the troubleshooting, use the **no** form of this command.

debug l4f {**api** | **flow-db** | **flows** | **packet** {**all** | **detail** | **injection** | **interception** | **proxying** | **spoofing**} | **test-app** | **trace-db-api** | **trace-db-flow** | **trace-engine**}

no debug l4f {**api** | **flow-db** | **flows** | **packet** {**all** | **detail** | **injection** | **interception** | **proxying** | **spoofing**} | **test-app** | **trace-db-api** | **trace-db-flow** | **trace-engine**}

Syntax Description

api	Toggles L4F API debugging.
flow-db	Toggles L4F flow database debugging.
flows	Toggles L4F flows debugging.
packet	Toggles L4F packet debugging.
all	Toggles all L4F packet debugging.
detail	Toggles L4F packet detail debugging.
injection	Toggles L4F packet injection debugging.
interception	Toggles L4F packet interception debugging.
proxying	Toggles L4F packet proxying debugging.
spoofing	Toggles L4F packet spoofing debugging.
test-app	Toggles L4F test application debugging.
trace-db-api	Toggles L4F database API debugging.
trace-db-flow	Toggles L4F database flow debugging.
trace-engine	Toggles L4F API tracing debugging.

Command Default

L4F debugging is off.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to enable debugging for L4F packets:

```
Router# debug l4f packet all
```

Usage Guidelines

Use this command to enable debugging for Layer 4 forwarding flows.

Related Commands

Command	Description
show l4f	Displays the flow database for L4F.

debug vpdn

To troubleshoot Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) virtual private dial-up network (VPDN) tunneling events and infrastructure, use the **debug vpdn** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

Note Effective with Cisco Release 12.4(11)T, the L2F protocol is not available in Cisco IOS software.

debug vpdn {**call** {**event** | **fsm**} | **authorization** {**error** | **event**} | **error** | **event** [**disconnect**] | **l2tp-sequencing** | **l2x-data** | **l2x-errors** | **l2x-events** | **l2x-packets** | **message** | **packet** [**detail** | **errors**] | **sss** {**error** | **event** | **fsm**} | **subscriber** {**error** | **event** | **fsm**}}

no debug vpdn {**call** {**event** | **fsm**} | **authorization** {**error** | **event**} | **error** | **event** [**disconnect**] | **l2tp-sequencing** | **l2x-data** | **l2x-errors** | **l2x-events** | **l2x-packets** | **message** | **packet** [**detail** | **errors**] | **sss** {**error** | **event** | **fsm**} | **subscriber** {**error** | **event** | **fsm**}}

Syntax Description

authorization error	Displays authorization errors.
authorization event	Displays authorization events.
call event	Displays significant events in the VPDN call manager.
call fsm	Displays significant events in the VPDN call manager finite state machine (fsm).
error	Displays VPDN errors.
event	Displays VPDN events.
disconnect	(Optional) Displays VPDN disconnect events.
l2tp-sequencing	Displays significant events related to L2TP sequence numbers such as mismatches, resend queue flushes, and drops.
l2x-data	Displays errors that occur in data packets.
l2x-errors	Displays errors that occur in protocol-specific conditions.
l2x-events	Displays events resulting from protocol-specific conditions.
l2x-packets	Displays detailed information about control packets in protocol-specific conditions.
message	Displays VPDN interprocess messages.
packet	Displays information about VPDN packets.
detail	(Optional) Displays detailed packet information, including packet dumps.
errors	(Optional) Displays errors that occur in packet processing.
sss error	Displays debug information about VPDN Subscriber Service Switch (SSS) errors. **Note** Effective with Cisco Release 12.4(20)T, the **debug vpdn sss error** command is not available in Cisco IOS software.
sss event	Displays debug information about VPDN SSS events. **Note** Effective with Cisco Release 12.4(20)T, the **debug vpdn sss event** command is not available in Cisco IOS software.

sss fsm	Displays debug information about the VPDN SSS fsm. **Note** Effective with Cisco Release 12.4(20)T, the **debug vpdn sss fsm** command is not available in Cisco IOS software.
subscriber error	Displays debug information about VPDN Subscriber errors.
subscriber event	Displays debug information about VPDN Subscriber events.
subscriber fsm	Displays debug information about the VPDN Subscriber fsm.

Command Modes

Privileged EXEC (#)

Command History

OS Release	Modification
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(31)S	The output was enhanced to display messages about control channel authentication events.
S Release	**Modification**
12.2(22)S	This command was integrated into Cisco IOS Release 12.2(22)S.
12.2(27)SBC	Support for enhanced display of messages about control channel authentication events was added in Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	Support for the display of messages about congestion avoidance events was added in Cisco IOS Release 12.2(28)SB.
12.2(31)SB	Support was added to decode the outbound control channel authentication events.
T Release	**Modification**
11.2	This command was introduced.
12.0(5)T	Support was added for L2TP debugging messages. The **l2tp-sequencing** and **error** keywords were added. The **l2f-errors**, **l2f-events**, and **l2f-packets** keywords were changed to **l2x-errors**, **l2x-events**, and **l2x-packets**.
12.2(4)T	Support was added for the **message** and **call** {**event** | **fsm**} keywords.
12.2(11)T	Support was added for the **detail** keyword.
12.2(13)T	Support was added for the **sss** {**error** | **event** | **fsm**} keywords.
12.3(14)T	Support was added to decode the outbound control channel authentication events.
12.4(15)T	Support was added for the **authorization** {**error** | **event**} keywords.
12.4(20)T	The **subscriber** keyword was added.
XE Release	**Modification**
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
Cisco IOS XE Release 2.6	This command was modified. Authentication failure messages for L2TPv3 were added.

Usage Guidelines

The **debug vpdn packet** and **debug vpdn packet detail** commands generate several debug operations per packet. Depending on the L2TP traffic pattern, these commands may cause the CPU load to increase to a high level that impacts performance.

Examples

This section contains the following examples:

- Debugging VPDN Events on a NAS—Normal L2F Operations
- Debugging VPDN Events on the Tunnel Server—Normal L2F Operations
- Debugging VPDN Events on the NAS—Normal L2TP Operations
- Debugging VPDN Events on the Tunnel Server—Normal L2TP Operations
- Debugging Protocol-Specific Events on the NAS—Normal L2F Operations
- Debugging Protocol-Specific Events on the Tunnel Server—Normal L2F Operations
- Displaying L2TP Congestion Avoidance Settings
- Debugging Errors on the NAS—L2F Error Conditions
- Debugging L2F Control Packets for Complete Information
- Debugging an L2TPv3 Xconnect Session—Normal Operations
- Debugging Control Channel Authentication Events

Debugging VPDN Events on a NAS—Normal L2F Operations

The network access server (NAS) has the following VPDN configuration:

```
vpdn-group 1
 request-dialin
  protocol l2f
  domain cisco.com
 initiate-to ip 172.17.33.125
username nas1 password nas1
```

The following is sample output from the **debug vpdn event** command on a NAS when an L2F tunnel is brought up and Challenge Handshake Authentication Protocol (CHAP) authentication of the tunnel succeeds:

```
Router# debug vpdn event

%LINK-3-UPDOWN: Interface Async6, changed state to up
*Mar 2 00:26:05.537: looking for tunnel -- cisco.com --
*Mar 2 00:26:05.545: Async6 VPN Forwarding...
*Mar 2 00:26:05.545: Async6 VPN Bind interface direction=1
*Mar 2 00:26:05.553: Async6 VPN vpn_forward_user user6@cisco.com is forwarded
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to up
*Mar 2 00:26:06.289: L2F: Chap authentication succeeded for nas1.
```

The following is sample output from the **debug vpdn event** command on a NAS when the L2F tunnel is brought down normally:

```
Router# debug vpdn event

%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to down
%LINK-5-CHANGED: Interface Async6, changed state to reset
*Mar 2 00:27:18.865: Async6 VPN cleanup
*Mar 2 00:27:18.869: Async6 VPN reset
*Mar 2 00:27:18.873: Async6 VPN Unbind interface
%LINK-3-UPDOWN: Interface Async6, changed state to down
```

Table 2 describes the significant fields shown in the two previous displays. The output describes normal operations when an L2F tunnel is brought up or down on a NAS.

Table 2 debug vpdn event Field Descriptions for the NAS

Field	Description
Asynchronous interface coming up	
%LINK-3-UPDOWN: Interface Async6, changed state to up	Asynchronous interface 6 came up.
looking for tunnel -- cisco.com -- Async6 VPN Forwarding...	Domain name is identified.
Async6 VPN Bind interface direction=1	Tunnel is bound to the interface. These are the direction values: • 1—From the NAS to the tunnel server • 2—From the tunnel server to the NAS
Async6 VPN vpn_forward_user user6@cisco.com is forwarded	Tunnel for the specified user and domain name is forwarded.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to up	Line protocol is up.
L2F: Chap authentication succeeded for nas1.	Tunnel was authenticated with the tunnel password nas1.
Virtual access interface coming down	
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to down	Normal operation when the virtual access interface is taken down.
Async6 VPN cleanup Async6 VPN reset Async6 VPN Unbind interface	Normal cleanup operations performed when the line or virtual access interface goes down.

Debugging VPDN Events on the Tunnel Server—Normal L2F Operations

The tunnel server has the following VPDN configuration, which uses nas1 as the tunnel name and the tunnel authentication name. The tunnel authentication name might be entered in a user's file on an authentication, authorization, and accounting (AAA) server and used to define authentication requirements for the tunnel.

```
vpdn-group 1
 accept-dialin
  protocol l2f
  virtual-template 1
 terminate-from hostname nas1
```

The following is sample output from the **debug vpdn event** command on the tunnel server when an L2F tunnel is brought up successfully:

```
Router# debug vpdn event

L2F: Chap authentication succeeded for nas1.
Virtual-Access3 VPN Virtual interface created for user6@cisco.com
Virtual-Access3 VPN Set to Async interface
Virtual-Access3 VPN Clone from Vtemplate 1 block=1 filterPPP=0
%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
Virtual-Access3 VPN Bind interface direction=2
Virtual-Access3 VPN PPP LCP accepted sent & rcv CONFACK
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to up
```

The following is sample output from the **debug vpdn event** command on a tunnel server when an L2F tunnel is brought down normally:

```
Router# debug vpdn event

%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to down
Virtual-Access3 VPN cleanup
Virtual-Access3 VPN reset
Virtual-Access3 VPN Unbind interface
Virtual-Access3 VPN reset
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to down
```

Table 3 describes the fields shown in two previous outputs. The output describes normal operations when an L2F tunnel is brought up or down on a tunnel server.

Table 3 debug vpdn event Field Descriptions for the Tunnel Server

Field	Description
Tunnel coming up	
L2F: Chap authentication succeeded for nas1.	PPP CHAP authentication status for the tunnel named nas1.
Virtual-Access3 VPN Virtual interface created for user6@cisco.com	Virtual access interface was set up on the tunnel server for the user user6@cisco.com.
Virtual-Access3 VPN Set to Async interface	Virtual access interface 3 was set to asynchronous for character-by-character transmission.
Virtual-Access3 VPN Clone from Vtemplate 1 block=1 filterPPP=0	Virtual template 1 was applied to virtual access interface 3.
%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up	Link status is set to up.

Table 3 debug vpdn event Field Descriptions for the Tunnel Server (continued)

Field	Description
Virtual-Access3 VPN Bind interface direction=2	Tunnel is bound to the interface. These are the direction values: • 1—From the NAS to the tunnel server • 2—From the tunnel server to the NAS
Virtual-Access3 VPN PPP LCP accepted sent & rcv CONFACK	PPP link control protocol (LCP) configuration settings (negotiated between the remote client and the NAS) were copied to the tunnel server and acknowledged.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to up	Line protocol is up; the line can be used.
Tunnel coming down	
%LINK-3-UPDOWN: Interface Virtual-Access3, changed state to down	Virtual access interface is coming down.
Virtual-Access3 VPN cleanup Virtual-Access3 VPN reset Virtual-Access3 VPN Unbind interface Virtual-Access3 VPN reset	Router is performing normal cleanup operations when a virtual access interface used for an L2F tunnel comes down.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access3, changed state to down	Line protocol is down for virtual access interface 3; the line cannot be used.

Debugging VPDN Events on the NAS—Normal L2TP Operations

The following is sample output from the **debug vpdn event** command on the NAS when an L2TP tunnel is brought up successfully:

```
Router# debug vpdn event

20:19:17: L2TP: I SCCRQ from ts1 tnl 8
20:19:17: L2X: Never heard of ts1
20:19:17: Tnl 7 L2TP: New tunnel created for remote ts1, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, ts1
20:19:17: Tnl 7 L2TP: Tunnel state change from idle to wait-ctl-reply
20:19:17: Tnl 7 L2TP: Got a Challenge Response in SCCCN from ts1
20:19:17: Tnl 7 L2TP: Tunnel Authentication success
20:19:17: Tnl 7 L2TP: Tunnel state change from wait-ctl-reply to established
20:19:17: Tnl 7 L2TP: SM State established
20:19:17: Tnl/Cl 7/1 L2TP: Session FS enabled
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/Cl 7/1 L2TP: New session created
20:19:17: Tnl/Cl 7/1 L2TP: O ICRP to ts1 8/1
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-connect to established
20:19:17: Vi1 VPDN: Virtual interface created for bum1@cisco.com
20:19:17: Vi1 VPDN: Set to Async interface
20:19:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
20:19:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
20:19:18: Vi1 VPDN: Bind interface direction=2
20:19:18: Vi1 VPDN: PPP LCP accepting rcv CONFACK
```

```
20:19:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
up
```

Debugging VPDN Events on the Tunnel Server—Normal L2TP Operations

The following is sample output from the **debug vpdn event** command on the tunnel server when an L2TP tunnel is brought up successfully:

```
Router# debug vpdn event

20:47:33: %LINK-3-UPDOWN: Interface Async7, changed state to up
20:47:35: As7 VPDN: Looking for tunnel -- cisco.com --
20:47:35: As7 VPDN: Get tunnel info for cisco.com with NAS nas1, IP 172.21.9.13
20:47:35: As7 VPDN: Forward to address 172.21.9.13
20:47:35: As7 VPDN: Forwarding...
20:47:35: As7 VPDN: Bind interface direction=1
20:47:35: Tnl/Cl 8/1 L2TP: Session FS enabled
20:47:35: Tnl/Cl 8/1 L2TP: Session state change from idle to wait-for-tunnel
20:47:35: As7 8/1 L2TP: Create session
20:47:35: Tnl 8 L2TP: SM State idle
20:47:35: Tnl 8 L2TP: Tunnel state change from idle to wait-ctl-reply
20:47:35: Tnl 8 L2TP: SM State wait-ctl-reply
20:47:35: As7 VPDN: bum1@cisco.com is forwarded
20:47:35: Tnl 8 L2TP: Got a challenge from remote peer, nas1
20:47:35: Tnl 8 L2TP: Got a response from remote peer, nas1
20:47:35: Tnl 8 L2TP: Tunnel Authentication success
20:47:35: Tnl 8 L2TP: Tunnel state change from wait-ctl-reply to established
20:47:35: Tnl 8 L2TP: SM State established
20:47:35: As7 8/1 L2TP: Session state change from wait-for-tunnel to wait-reply
20:47:35: As7 8/1 L2TP: Session state change from wait-reply to established
20:47:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, changed state to up
```

Debugging Protocol-Specific Events on the NAS—Normal L2F Operations

The following is sample output from the **debug vpdn l2x-events** command on the NAS when an L2F tunnel is brought up successfully:

```
Router# debug vpdn l2x-events

%LINK-3-UPDOWN: Interface Async6, changed state to up
*Mar 2 00:41:17.365: L2F Open UDP socket to 172.21.9.26
*Mar 2 00:41:17.385: L2F_CONF received
*Mar 2 00:41:17.389: L2F Removing resend packet (type 1)
*Mar 2 00:41:17.477: L2F_OPEN received
*Mar 2 00:41:17.489: L2F Removing resend packet (type 2)
*Mar 2 00:41:17.493: L2F building nas2gw_mid0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to up
*Mar 2 00:41:18.613: L2F_OPEN received
*Mar 2 00:41:18.625: L2F Got a MID management packet
*Mar 2 00:41:18.625: L2F Removing resend packet (type 2)
*Mar 2 00:41:18.629: L2F MID synced NAS/HG Clid=7/15 Mid=1 on Async6
```

The following is sample output from the **debug vpdn l2x-events** command on a NAS when an L2F tunnel is brought down normally:

```
Router# debug vpdn l2x-events

%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to down
%LINK-5-CHANGED: Interface Async6, changed state to reset
*Mar 2 00:42:29.213: L2F_CLOSE received
*Mar 2 00:42:29.217: L2F Destroying mid
*Mar 2 00:42:29.217: L2F Removing resend packet (type 3)
*Mar 2 00:42:29.221: L2F Tunnel is going down!
```

```
*Mar 2 00:42:29.221: L2F Initiating tunnel shutdown.
*Mar 2 00:42:29.225: L2F_CLOSE received
*Mar 2 00:42:29.229: L2F_CLOSE received
*Mar 2 00:42:29.229: L2F Got closing for tunnel
*Mar 2 00:42:29.233: L2F Removing resend packet
*Mar 2 00:42:29.233: L2F Closed tunnel structure
%LINK-3-UPDOWN: Interface Async6, changed state to down
*Mar 2 00:42:31.793: L2F Closed tunnel structure
*Mar 2 00:42:31.793: L2F Deleted inactive tunnel
```

Table 4 describes the fields shown in the displays.

Table 4 debug vpdn l2x-events Field Descriptions—NAS

Field	Descriptions
Tunnel coming up	
%LINK-3-UPDOWN: Interface Async6, changed state to up	Asynchronous interface came up normally.
L2F Open UDP socket to 172.21.9.26	L2F opened a User Datagram Protocol (UDP) socket to the tunnel server IP address.
L2F_CONF received	L2F_CONF signal was received. When sent from the tunnel server to the NAS, an L2F_CONF indicates the tunnel server's recognition of the tunnel creation request.
L2F Removing resend packet (type ...)	Removing the resend packet for the L2F management packet. There are two resend packets that have different meanings in different states of the tunnel.
L2F_OPEN received	L2F_OPEN management message was received, indicating that the tunnel server accepted the NAS configuration of an L2F tunnel.
L2F building nas2gw_mid0	L2F is building a tunnel between the NAS and the tunnel server using the multiplex ID (MID) MID0.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to up	Line protocol came up. Indicates whether the software processes that handle the line protocol regard the interface as usable.
L2F_OPEN received	L2F_OPEN management message was received, indicating that the tunnel server accepted the NAS configuration of an L2F tunnel.
L2F Got a MID management packet	MID management packets are used to communicate between the NAS and the tunnel server.
L2F MID synced NAS/HG Clid=7/15 Mid=1 on Async6	L2F synchronized the client IDs on the NAS and the tunnel server, respectively. An MID is assigned to identify this connection in the tunnel.
Tunnel coming down	
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to down	Line protocol came down. Indicates whether the software processes that handle the line protocol regard the interface as usable.

Table 4 debug vpdn l2x-events Field Descriptions—NAS (continued)

Field	Descriptions
%LINK-5-CHANGED: Interface Async6, changed state to reset	Interface was marked as reset.
L2F_CLOSE received	NAS received a request to close the tunnel.
L2F Destroying mid	Connection identified by the MID is being taken down.
L2F Tunnel is going down!	Advisory message about impending tunnel shutdown.
L2F Initiating tunnel shutdown.	Tunnel shutdown has started.
L2F_CLOSE received	NAS received a request to close the tunnel.
L2F Got closing for tunnel	NAS began tunnel closing operations.
%LINK-3-UPDOWN: Interface Async6, changed state to down	Asynchronous interface was taken down.
L2F Closed tunnel structure	NAS closed the tunnel.
L2F Deleted inactive tunnel	Now-inactivated tunnel was deleted.

Debugging Protocol-Specific Events on the Tunnel Server—Normal L2F Operations

The following is sample output from the **debug vpdn l2x-events** command on a tunnel server when an L2F tunnel is created:

```
Router# debug vpdn l2x-events

L2F_CONF received
L2F Creating new tunnel for nas1
L2F Got a tunnel named nas1, responding
L2F Open UDP socket to 172.21.9.25
L2F_OPEN received
L2F Removing resend packet (type 1)
L2F_OPEN received
L2F Got a MID management packet
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

The following is sample output from the **debug vpdn l2x-events** command on a tunnel server when the L2F tunnel is brought down normally:

```
Router# debug vpdn l2x-events

L2F_CLOSE received
L2F Destroying mid
L2F Removing resend packet (type 3)
L2F Tunnel is going down!
L2F Initiating tunnel shutdown.
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
L2F_CLOSE received
L2F Got closing for tunnel
L2F Removing resend packet
L2F Removing resend packet
L2F Closed tunnel structure
L2F Closed tunnel structure
L2F Deleted inactive tunnel
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
```

Table 5 describes the significant fields shown in the displays.

Table 5 debug vpdn l2x-events Field Descriptions—Tunnel Server

Field	Description
Tunnel coming up	
L2F_CONF received	L2F configuration is received from the NAS. When sent from a NAS to a tunnel server, the L2F_CONF is the initial packet in the conversation.
L2F Creating new tunnel for nas1	Tunnel named nas1 is being created.
L2F Got a tunnel named nas1, responding	Tunnel server is responding.
L2F Open UDP socket to 172.21.9.25	Opening a socket to the NAS IP address.
L2F_OPEN received	L2F_OPEN management message was received, indicating that the NAS is opening an L2F tunnel.
L2F Removing resend packet (type 1)	Removing the resend packet for the L2F management packet. The two resend packet types have different meanings in different states of the tunnel.
L2F Got a MID management packet	L2F MID management packets are used to communicate between the NAS and the tunnel server.
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up	Tunnel server is bringing up virtual access interface 1 for the L2F tunnel.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up	Line protocol is up. The line can be used.
Tunnel coming down	
L2F_CLOSE received	NAS or tunnel server received a request to close the tunnel.
L2F Destroying mid	Connection identified by the MID is being taken down.
L2F Removing resend packet (type 3)	Removing the resend packet for the L2F management packet. There are two resend packets that have different meanings in different states of the tunnel.
L2F Tunnel is going down! L2F Initiating tunnel shutdown.	Router is performing normal operations when a tunnel is coming down.
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down	The virtual access interface is coming down.

Table 5 debug vpdn l2x-events Field Descriptions—Tunnel Server (continued)

Field	Description
L2F_CLOSE received L2F Got closing for tunnel L2F Removing resend packet L2F Removing resend packet L2F Closed tunnel structure L2F Closed tunnel structure L2F Deleted inactive tunnel	Router is performing normal cleanup operations when the tunnel is being brought down.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down	Line protocol is down; virtual access interface 1 cannot be used.

Displaying L2TP Congestion Avoidance Settings

The following partial example of the **debug vpdn l2x-events** command is useful for monitoring a network running the L2TP Congestion Avoidance feature. The report shows that the congestion window (CWND) window has been reset to 1 because of packet retransmissions:

```
Router# debug vpdn l2x-events
.
.
.
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Congestion Control event received is retransmission
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Congestion Window size, Cwnd 1
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Slow Start threshold, Ssthresh 2
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Remote Window size, 500
*Jul 15 19:02:57.963:  Tnl 47100 L2TP: Control channel retransmit delay set to 4 seconds
*Jul 15 19:03:01.607:  Tnl 47100 L2TP: Update ns/nr, peer ns/nr 2/5, our ns/nr 5/2
```

The following partial example shows that traffic has been restarted with L2TP congestion avoidance throttling traffic:

```
Router# debug vpdn l2x-events
.
.
.
*Jul 15 14:45:16.123:  Tnl 30597 L2TP: Control channel retransmit delay set to 2 seconds
*Jul 15 14:45:16.123:  Tnl 30597 L2TP: Tunnel state change from idle to wait-ctl-reply
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Control event received is positive
acknowledgement
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Window size, Cwnd 2
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Slow Start threshold, Ssthresh 500
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Remote Window size, 500
*Jul 15 14:45:16.131:  Tnl 30597 L2TP: Congestion Ctrl Mode is Slow Start
```

Table 6 briefly describes the significant fields shown in the displays. See RFC 2661 for more details about the information in the reports for L2TP congestion avoidance.

Table 6 debug vpdn l2x-events Field Descriptions—L2TP Congestion Avoidance

Field	Description
Control channel retransmit delay set to ...	Indicates the current value set for the retransmit delay.
Tunnel state...	Indicates the tunnel's current Control Connection State, per RFC 2661.
Congestion Control event received is...	Indicates the received congestion control event. • Retransmission—Indicates packet retransmission has been detected in the resend queue. • Positive acknowledgement—Indicates that a packet was received and acknowledged by the peer tunnel endpoint.
Congestion Window size, Cwnd 2	Current size of the congestion window (Cwnd).
Slow Start threshold, Ssthresh 500	Current value of the slow start threshold (Ssthresh).
Remote Window size, 500	Size of the advertised receive window configured on the remote peer with the **l2tp tunnel receive-window** command.
Congestion Ctrl Mode is...	Indicates whether the router is operating in Slow Start or Congestion Avoidance mode.
Update ns/nr, peer ns/nr 2/5, our ns/nr 5/2	See RFC 2661.

Debugging Errors on the NAS—L2F Error Conditions

The following is sample output from the **debug vpdn error** command on a NAS when the L2F tunnel is not set up:

```
Router# debug vpdn error

%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to down
%LINK-5-CHANGED: Interface Async1, changed state to reset
%LINK-3-UPDOWN: Interface Async1, changed state to down
%LINK-3-UPDOWN: Interface Async1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
VPDN tunnel management packet failed to authenticate
VPDN tunnel management packet failed to authenticate
```

Table 7 describes the significant fields shown in the display.

Table 7 debug vpdn error Field Descriptions for the NAS

Field	Description
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to down	Line protocol on the asynchronous interface went down.
%LINK-5-CHANGED: Interface Async1, changed state to reset	Asynchronous interface 1 was reset.

Table 7 debug vpdn error Field Descriptions for the NAS (continued)

Field	Description
%LINK-3-UPDOWN: Interface Async1, changed state to down %LINK-3-UPDOWN: Interface Async1, changed state to up	Link from asynchronous interface 1 link went down and then came back up.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up	Line protocol on the asynchronous interface came back up.
VPDN tunnel management packet failed to authenticate	Tunnel authentication failed. This is the most common VPDN error. **Note** Verify the password for the NAS and the tunnel server name. If you store the password on an AAA server, you can use the **debug aaa authentication** command.

The following is sample output from the **debug vpdn l2x-errors** command:

```
Router# debug vpdn l2x-errors

%LINK-3-UPDOWN: Interface Async1, changed state to up
L2F Out of sequence packet 0 (expecting 0)
L2F Tunnel authentication succeeded for cisco.com
 L2F Received a close request for a non-existent mid
 L2F Out of sequence packet 0 (expecting 0)
 L2F packet has bogus1 key 1020868 D248BA0F
L2F packet has bogus1 key 1020868 D248BA0F
```

Table 8 describes the significant fields shown in the display.

Table 8 debug vpdn l2x-errors Field Descriptions

Field	Description
%LINK-3-UPDOWN: Interface Async1, changed state to up	The line protocol on the asynchronous interface came up.
L2F Out of sequence packet 0 (expecting 0)	Packet was expected to be the first in a sequence starting at 0, but an invalid sequence number was received.
L2F Tunnel authentication succeeded for cisco.com	Tunnel was established from the NAS to the tunnel server, cisco.com.
L2F Received a close request for a non-existent mid	Multiplex ID was not used previously; cannot close the tunnel.
L2F Out of sequence packet 0 (expecting 0)	Packet was expected to be the first in a sequence starting at 0, but an invalid sequence number was received.
L2F packet has bogus1 key 1020868 D248BA0F	Value based on the authentication response given to the peer during tunnel creation. This packet, in which the key does not match the expected value, must be discarded.
L2F packet has bogus1 key 1020868 D248BA0F	Another packet was received with an invalid key value. The packet must be discarded.

Debugging L2F Control Packets for Complete Information

The following is sample output from the **debug vpdn l2x-packets** command on a NAS. This example displays a trace for a **ping** command.

```
Router# debug vpdn l2x-packets

L2F SENDING (17): D0 1 1 10 0 0 0 4 0 11 0 0 81 94 E1 A0 4
L2F header flags: 53249 version 53249 protocol 1 sequence 16 mid 0 cid 4
length 17 offset 0 key 1701976070
L2F RECEIVED (17): D0 1 1 10 0 0 0 4 0 11 0 0 65 72 18 6 5
L2F SENDING (17): D0 1 1 11 0 0 0 4 0 11 0 0 81 94 E1 A0 4
L2F header flags: 53249 version 53249 protocol 1 sequence 17 mid 0 cid 4
length 17 offset 0 key 1701976070
L2F RECEIVED (17): D0 1 1 11 0 0 0 4 0 11 0 0 65 72 18 6 5
L2F header flags: 57345 version 57345 protocol 2 sequence 0 mid 1 cid 4
length 32 offset 0 key 1701976070
L2F-IN Output to Async1 (16): FF 3 C0 21 9 F 0 C 0 1D 41 AD FF 11 46 87
L2F-OUT (16): FF 3 C0 21 A F 0 C 0 1A C9 BD FF 11 46 87
L2F header flags: 49153 version 49153 protocol 2 sequence 0 mid 1 cid 4
length 32 offset 0 key -2120949344
L2F-OUT (101): 21 45 0 0 64 0 10 0 0 FF 1 B9 85 1 0 0 3 1 0 0 1 8 0 62 B1
0 0 C A8 0 0 0 0 0 11 E E0 AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD
AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB
CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD
L2F header flags: 49153 version 49153 protocol 2 sequence 0 mid 1 cid 4
length 120 offset 3 key -2120949344
L2F header flags: 49153 version 49153 protocol 2 sequence 0 mid 1 cid 4
length 120 offset 3 key 1701976070
L2F-IN Output to Async1 (101): 21 45 0 0 64 0 10 0 0 FF 1 B9 85 1 0 0 1 1 0
0 3 0 0 6A B1 0 0 C A8 0 0 0 0 0 11 E E0 AB CD AB CD AB CD AB CD AB CD AB CD
AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB
CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD AB CD
```

Table 9 describes the significant fields shown in the display.

Table 9 debug vpdn l2x-packets Field Descriptions

Field	Description
L2F SENDING (17)	Number of bytes being sent. The first set of "SENDING"..."RECEIVED" lines displays L2F keepalive traffic. The second set displays L2F management data.
L2F header flags:	Version and flags, in decimal.
version 53249	Version.
protocol 1	Protocol for negotiation of the point-to-point link between the NAS and the tunnel server is always 1, indicating L2F management.
sequence 16	Sequence numbers start at 0. Each subsequent packet is sent with the next increment of the sequence number. The sequence number is thus a free running counter represented modulo 256. There is a distinct sequence counter for each distinct MID value.
mid 0	MID, which identifies a particular connection within the tunnel. Each new connection is assigned a MID currently unused within the tunnel.
cid 4	Client ID used to assist endpoints in demultiplexing tunnels.
length 17	Size in octets of the entire packet, including header, all fields pre-sent, and payload. Length does not reflect the addition of the checksum, if present.

Table 9 debug vpdn l2x-packets Field Descriptions (continued)

Field	Description
offset 0	Number of bytes past the L2F header at which the payload data is expected to start. If it is 0, the first byte following the last byte of the L2F header is the first byte of payload data.
key 1701976070	Value based on the authentication response given to the peer during tunnel creation. During the life of a session, the key value serves to resist attacks based on spoofing. If a packet is received in which the key does not match the expected value, the packet must be silently discarded.
L2F RECEIVED (17)	Number of bytes received.
L2F-IN Otput to Async1 (16)	Payload datagram. The data came in to the VPDN code.
L2F-OUT (16):	Payload datagram sent out from the VPDN code to the tunnel.
L2F-OUT (101)	Ping payload datagram. The value 62 in this line is the ping packet size in hexadecimal (98 in decimal). The three lines that follow this line show ping packet data.

Debugging an L2TPv3 Xconnect Session—Normal Operations

The following example shows output from the **debug vpdn l2x-events** command for an L2TP version 3 (L2TPv3) xconnect session on an Ethernet interface:

```
Router# debug vpdn l2x-events

23:31:18: L2X: l2tun session [1669204400], event [client request], old state [open], new
state [open]
 23:31:18: L2X: L2TP: Received L2TUN message <Connect>
 23:31:18: Tnl/Sn58458/28568 L2TP: Session state change from idle to wait-for-tunnel
 23:31:18: Tnl/Sn58458/28568 L2TP: Create session
 23:31:18: Tnl58458 L2TP: SM State idle
 23:31:18: Tnl58458 L2TP: O SCCRQ
 23:31:18: Tnl58458 L2TP: Control channel retransmit delay set to 1 seconds
 23:31:18: Tnl58458 L2TP: Tunnel state change from idle to wait-ctl-reply
 23:31:18: Tnl58458 L2TP: SM State wait-ctl-reply
 23:31:18: Tnl58458 L2TP: I SCCRP from router
 23:31:18: Tnl58458 L2TP: Tunnel state change from wait-ctl-reply to established
 23:31:18: Tnl58458 L2TP: O SCCCN to router tnlid 8012
 23:31:18: Tnl58458 L2TP: Control channel retransmit delay set to 1 seconds
 23:31:18: Tnl58458 L2TP: SM State established
 23:31:18: Tnl/Sn58458/28568 L2TP: O ICRQ to router 8012/0
 23:31:18: Tnl/Sn58458/28568 L2TP: Session state change from wait-for-tunnel to wait-reply
 23:31:19: Tnl58458 L2TP: Control channel retransmit delay set to 1 seconds
 23:31:20: %LINK-3-UPDOWN: Interface Ethernet2/1, changed state to up
 23:31:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/1, changed state to
up
 23:31:25: L2X: Sending L2TUN message <Connect OK>
 23:31:25: Tnl/Sn58458/28568 L2TP: O ICCN to router 8012/35149
 23:31:25: Tnl58458 L2TP: Control channel retransmit delay set to 1 seconds
 23:31:25: Tnl/Sn58458/28568 L2TP: Session state change from wait-reply to established
 23:31:25: L2X: l2tun session [1669204400], event [server response], old state [open], new
state [open]
 23:31:26: Tnl58458 L2TP: Control channel retransmit delay set to 1 seconds
```

Debugging Control Channel Authentication Events

The following debug messages show control channel authentication failure events in Cisco IOS Release 12.0(31)S:

```
Router# debug vpdn l2x-events

!
Tnl41855 L2TP: Per-Tunnel auth counter, Overall Failed, now 1
Tnl41855 L2TP: Tunnel auth counter, Overall Failed, now 219
!
```

Related Commands

Command	Description
debug aaa authentication	Displays information on AAA/TACACS+ authentication.
debug acircuit	Displays events and failures related to attachment circuits.
debug pppoe	Display debugging information for PPPoE sessions.
debug vpdn pppoe-data	Displays data packets of PPPoE sessions.
debug vpdn pppoe-error	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established sessions to be closed.
debug vpdn pppoe-events	Displays PPPoE protocol messages about events that are part of normal session establishment or shutdown.
debug vpdn pppoe-packet	Displays each PPPoE protocol packet exchanged.
debug xconnect	Displays errors and events related to an xconnect configuration.

debug waas

To display debugging information about WAAS Express modules, use the **debug waas** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug waas {**auto-discovery** | **aoim** | **cce** | **dre** | **infrastructure** | **lz** | **memory** | **management** | **tfo**} {**events** | **errors** | **operations** [**brief**]}

no debug waas {**auto-discovery** | **aoim** | **cce** | **dre** | **infrastructure** | **lz** | **memory** | **management** | **tfo**} {**events** | **errors** | **operations** [**brief**]}

Syntax Description

auto-discovery	Displays autodiscovery information about WAAS Express.
aoim	Displays peer information and negotiated capabilities information.
cce	Displays CCE information.
dre	Displays information about Data Redundancy Elimination (DRE) optimization.
infrastructure	Displays information about the WAAS Express infrastructure.
lz	Displays information about Lempel-Ziv (LZ) optimization.
memory	Displays information about WAAS Express internal memory usage.
tfo	Displays information about TCP Flow Optimization (TFO).
brief	Displays WAAS connection operations in brief.
event	Displays information about events.
error	Displays information about errors.
operations	Displays information about operations.
management	Displays information about error and event management.

Command Default

Debugging information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display debugging information about WAAS Express.

Examples

The following example shows how to enable debugging output in brief for WAAS Express infrastructure operations:

```
Router> enable
Router# debug waas infrastructure operations brief
```

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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.

digest

To enable Layer 2 Tunneling Protocol Version 3 (L2TPv3) control channel authentication or integrity checking, use the **digest** command in L2TP class configuration mode. To disable control channel authentication or integrity checking, use the **no** form of this command.

digest [**secret** [**0** | **7**] *password*] [**hash** {**md5** | **sha**}]

no digest [**secret** [**0** | **7**] *password* [**hash** {**md5** | **sha**}]]

Syntax Description

secret	(Optional) Enables L2TPv3 control channel authentication. If the **digest** command is issued without the **secret** keyword option, L2TPv3 integrity checking will be enabled.
[**0** | **7**]	Specifies the input format of the shared secret. • **0**—Specifies that a plain-text secret will be entered. • **7**—Specifies that an encrypted secret will be entered. The default value is **0**.
password	The shared secret used between peer provider edge (PE) routers. The value entered for the *password* argument must be in the format that matches the input format specified by the [**0** | **7**] keyword option.
hash {**md5** | **sha**}	(Optional) Specifies the hash function to be used in per-message digest calculations. • **md5**—Specifies HMAC-MD5 hashing. • **sha**—Specifies HMAC-SHA-1 hashing. The default hash function is **md5**.

Command Default

L2TPv3 control channel authentication and integrity checking are disabled by default.

Command Modes

L2TP class configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.0(30)S	This command was enhanced to allow two different passwords to be configured simultaneously.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

Beginning in Cisco IOS Release 12.0(29)S, two methods of control channel authentication are available. The L2TPv3 Control Message Hashing feature (enabled with the **digest** command) introduces a more robust authentication method than the older Challenge Handshake Authentication Protocol (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.

Table 10 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 10 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	None
		New integrity check	New integrity check
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	None
		New integrity check	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.

In Cisco IOS Release 12.0(30)S, this command was enhanced to allow two L2TPv3 control channel authentication passwords to be configured simultaneously. This enhancement allows the transition from using an old authentication password to using a new authentication password without interrupting L2TPv3 services. No more than two passwords may be configured at a time. In order to configure a new password when two passwords are already configured, you must remove one of the existing passwords using the **no digest secret** *password* command. The number of configured passwords can be verified using the **show l2tun tunnel** command.

Examples

The following example configures control channel authentication and a control channel authentication password for tunnels belonging to the L2TP class named class1:

```
l2tp-class class1
 digest secret cisco hash sha
 hidden
```

The following example configures a second control channel authentication password for tunnels belonging to the L2TP class named class1:

```
l2tp-class class1
 digest secret cisco2 hash sha
```

The following example removes the old control channel authentication password for tunnels belonging to the L2TP class named class1. The old password should be removed only after all peer routers have been configured with the new password.

```
l2tp-class class1
 no digest secret cisco hash sha
```

The following example configures control channel integrity checking and disables validation of the message digest for L2TPv3 tunnels belonging to the L2TP class named class2:

```
l2tp-class class2
 digest hash sha
 no digest check
```

The following example disables validation of the message digest for L2TPv3 tunnels belonging to the L2TP class named class3. Control channel authentication and control channel integrity checking are both disabled.

```
l2tp-class class3
 no digest check
```

Related Commands

Command	Description
authentication	Enables L2TPv3 CHAP-style authentication.
digest check	Enables the validation of the message digest in received control messages.
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.
show l2tun tunnel	Displays the current state of L2TPv3 tunnels and displays information about currently configured tunnels, including local and remote L2TP hostnames, aggregate packet counts, and L2TP control channels.

dscp (Frame Relay VC-bundle-member)

To configure the differentiated services code point (DSCP) levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **dscp** command in Frame Relay VC-bundle-member configuration mode. To remove the DSCP level configuration from the PVC, use the **no** form of this command.

dscp {*level* | **other**}

no dscp *level*

Syntax Description

level	DSCP level or levels for the Frame Relay PVC bundle member. The range is from 0 to 63. A PVC bundle member can be configured with a single DSCP level, multiple individual DSCP levels, a range of DSCP levels, multiple ranges of DSCP levels, or a combination of individual levels and level ranges. For example: • 9 • 25,35,45 • 25-35,45-55 • 10,20,25-35,40,45-55,60
other	Specifies that the Frame Relay PVC bundle member will handle all of the remaining DSCP levels that are not specified by other PVC bundle members.

Command Default

DSCP levels are not configured.

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.
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

Assignment of DSCP levels to PVC bundle members lets you create differentiated service, because you can distribute the DSCP levels over the various PVC bundle members. You can map a single DSCP level or range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different DSCP levels.

Use the **dscp other** command to configure a PVC to carry traffic marked with DSCP levels not specifically configured on other PVCs. Only one PVC in the bundle can be configured with the **dscp other** command.

This command is available only when the match type for the PVC bundle is set to **dscp** by using the **match dscp** command in Frame Relay VC-bundle configuration mode.

You can overwrite the DSCP level configuration on a PVC by reentering the **dscp** command with a new level value.

There is no default value for this command. When the PVC bundle is set to **dscp** using the **match dscp** command, all PVCs in the bundle are reset to remove any existing DSCP values. If one or more DSCP values are not specifically configured, the bundle will not come up.

However, a PVC may exist in a bundle but have no DSCP value associated with the bundle. As long as all valid DSCP values are handled by one or more of the other PVCs in the bundle, the bundle can come up, but the PVC that has no DSCP value configured will not participate in the bundle.

A DSCP level can be configured on one PVC bundle member per bundle. If you configure the same DSCP level on more than one PVC within a bundle, the following error warning appears on the console:

```
%Overlapping diff-serv code points
```

Examples

The following example assigns DSCP levels 0 through 9 to PVC bundle member 300 in a Frame Relay PVC bundle named MP-3-static:

```
interface Serial4/0
 encapsulation frame-relay
 frame-relay vc-bundle MP-3-static
  match dscp
  pvc 300
   dscp 0-9

 frame-relay map ip 10.2.2.2 vc-bundle MP-3-static
```

The following example changes the DSCP levels in the above example from 0 through 9 to 0, 9, and 20 through 29:

```
interface serial 1/4
 frame-relay map ip 10.2.2.2 vc-bundle MP-3-static
 frame-relay vc-bundle MP-3-static
  match dscp
  pvc 300
   dscp 0,9,20-29
```

Related Commands

Command	Description
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
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.
match	Specifies which bits in the ToS octet to use for mapping packet service levels to Frame Relay PVC bundle members.

Command	Description
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
pvc (Frame Relay VC-bundle)	Creates a PVC and PVC bundle member and enters Frame Relay VC-bundle-member configuration mode.

efci-bit

To set the explicit forward congestion indication (EFCI) bit field in the ATM cell header for FRF.8 service interworking, use the **efci-bit** command in FRF.8 connect mode. To disable or reset this bit, use the **no** form of this command.

efci-bit {**0** | **map-fecn**}

no efci-bit {**0** | **map-fecn**}

Syntax Description

0	The EFCI field in the ATM cell header is set to 0.
map-fecn	The EFCI field in the ATM cell header is set to 1 when the forward explicit congestion notification (FECN) field in the Frame Relay header is set.

Defaults

The default is **0**.

Command Modes

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

The following example creates a connection that connects Frame Relay DLCI 100 to ATM PVC 0/32, and sets the EFCI field in the ATM cell header to 1 when the FECN field in the Frame Relay header is set:

```
Router(config)# interface atm1/0
Router(config-if)# pvc 0/32
Router(config-if)# encapsulation aal5mux fr-atm-srv
Router(config)# connect 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.
connect (FRF.8)	Connects a Frame Relay DLCI to an ATM PVC.
connect (FRF.5)	Sets the Frame Relay DE bit field in the Frame Relay cell header.
service translation	Allows mapping between encapsulated ATM PDUs and encapsulated Frame Relay PDUs.

encapsulation (Any Transport over MPLS)

To configure the ATM adaptation layer (AAL) encapsulation for an Any Transport over MPLS (AToM), use the **encapsulation** command in the appropriate configuration mode. To remove the ATM encapsulation, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	The adaptation layer type, which is one of the following: • **aal5**—ATM adaptation layer 5 • **aal0**—ATM adaptation layer 0

Command Default

The default encapsulation is AAL5.

Command Modes

L2transport VC configuration—for ATM PVCs
VC class configuration—for VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
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.
12.0(30)S	This command was updated to enable ATM encapsulations 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

In L2transport VC configuration mode, the **pvc** command and the **encapsulation** command work together. Use the commands for AToM differently than for all other applications. Table 11 shows the differences in how the commands are used.

Table 11 AToM-Specific Variations of the pvc and encapsulation Commands

Other Applications	AToM
`Router(config-if)# pvc 1/100` `Router(config-if-atm-vc)# encapsulation aal5snap`	`Router(config-if)# pvc 1/100 l2transport` `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`

The following list highlights the differences:

- **pvc** command: For most applications, you create a permanent virtual circuit (PVC) by using the **pvc** *vpi/vci* command. For AToM, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- **encapsulation** command: The **encapsulation** command for AToM has only two keyword values: **aal5** or **aal0**. You cannot specify an encapsulation type, such as **aal5snap**. In contrast, the **encapsulation aal5** command you use for most other applications requires you to specify the encapsulation type, such as **aal5snap**.
- You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets.

When you use the **aal5** keyword, incoming cells (except Operation, Administration, and Maintenance [OAM] cells) on that PVC are treated as AAL5 encapsulated packets. The router reassembles the packet from the incoming cells. The router does not check the contents of the packet, so it does not need to know the encapsulation type (such as **aal5snap** and **aal5mux**). After imposing the Multiprotocol Label Switching (MPLS) label stack, the router sends the reassembled packet over the MPLS core network.

When you use the **aal0** keyword, the router strips the header error control (HEC) byte from the cell header and adds the MPLS label stack. The router sends the cell over the MPLS core network.

Examples

The following example shows how to configure a PVC to transport ATM cell relay packets for AToM:

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# pvc 1/100 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over MPLS in VC class configuration mode. The VC class is applied to a PVC.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
Router(config)# interface atm1/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# class-vc aal5class
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation (Frame Relay VC-bundle)

To override the encapsulation for a point-to-point subinterface and configure Frame Relay encapsulation for an individual Frame Relay permanent virtual circuit (PVC) bundle, use the **encapsulation** command in Frame Relay VC-bundle configuration mode. To disable the encapsulation for the individual PVC bundle and revert to the encapsulation for the point-to-point subinterface, use the **no** form of this command.

encapsulation [**cisco** | **ietf**]

no encapsulation [**cisco** | **ietf**]

Syntax Description

cisco	(Optional) Uses Cisco proprietary encapsulation, which is a four-byte header, with two bytes to identify the data-link connection identifier (DLCI) and two bytes to identify the packet type
ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490 and RFC 2427). Use this keyword when connecting to another vendor's equipment across a Frame Relay network on point-to-point interfaces.

Defaults

Encapsulation type that is configured on the main interface.

Command Modes

Frame Relay VC-bundle configuration

Command History

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

Usage Guidelines

Use this command to override the encapsulation at a point-to-point subinterface for an individual Frame Relay PVC bundle. This command is available for point-to-point subinterfaces only; it cannot be used on multipoint interfaces.

Examples

The following example configures RFC 1490 encapsulation for the Frame Relay PVC bundle named "P2P-5":

```
interface serial 1/4.2 point-to-point
 ip address 10.1.1.1 255.0.0.0
 frame-relay vc-bundle P2P-5
  encapsulation ietf
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation on an interface.

encapsulation (L2TP)

To specify the Layer 2 data encapsulation method to be used for tunneling IP traffic over a pseudowire, use the **encapsulation** (L2TP) command in pseudowire class configuration mode. To remove the specified Layer 2 encapsulation method, use the **no** form of this command.

encapsulation {**l2tpv2** | **l2tpv3** [**manual**] | **mpls**}

no encapsulation {**l2tpv2** | **l2tpv3** [**manual**] | **mpls**}

Syntax Description

l2tpv2	Uses Layer 2 Tunneling Protocol (L2TP) as the tunneling method to encapsulate data in the pseudowire.
l2tpv3	Uses Layer 2 Tunneling Protocol Version 3 (L2TPv3) as the tunneling method to encapsulate data in the pseudowire.
manual	(Optional) No signaling is to be used in the L2TPv3 control channel.
mpls	Uses Multiprotocol Label Switching (MPLS) as the tunneling method to encapsulate data in the pseudowire.

Defaults

No encapsulation method is specified.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	The **l2tpv2** keyword was added and this command was integrated into Cisco IOS Release 12.3(2)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

This command must be configured if the pseudowire class will be referenced from an xconnect or pseudowire configured to forward Layer 2 traffic.

Examples

The following example shows how to configure L2TPv3 as the data encapsulation method for the pseudowire class named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation l2tpv3
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

encapsulation (Layer 2 local switching)

To configure the ATM adaptation layer (AAL) for a Layer 2 local switching ATM permanent virtual circuit (PVC), use the **encapsulation** command in ATM PVC L2transport configuration mode. To remove an encapsulation from a PVC, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	Adaptation layer type. The values are: • **aal5** • **aal0** • **aal5snap** • **aal5mux** • **aal5nlpid** (not available on Cisco 12000 series)

Command Default

If you do not create a PVC, one is created for you. The default encapsulation types for autoprovisioned PVCs are as follows:

- For ATM-to-ATM local switching, the default encapsulation type for the PVC is AAL0.
- For ATM-to-Ethernet or ATM-to-Frame Relay local switching, the default encapsulation type for the PVC is AAL5 SNAP.

Command Modes

ATM PVC L2transport configuration

Command History

Release	Modification
12.0(27)S	This command was introduced for Layer 2 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.

Usage Guidelines

The **pvc** command and the **encapsulation** command work together. The use of these commands with Layer 2 local switching is slightly different from the use of these commands with other applications. The following list highlights the differences:

- For Layer 2 local switching, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- The Layer 2 local switching **encapsulation** command works only with the **pvc** command. You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets. You can use only PVCs to transport Layer 2 packets.

Table 12 shows the encapsulation types supported for each transport type:

Table 12 Supported Encapsulation Types

Interworking Type	Encapsulation Type
ATM to ATM	AAL0, AAL5
ATM to Ethernet with IP interworking	AAL5SNAP, AAL5MUX
ATM to Ethernet with Ethernet interworking	AAL5SNAP
ATM to Frame-Relay	AAL5SNAP, AAL5NLPID

Examples

The following example shows how to configure a PVC to transport AAL0 packets for Layer 2 local switching:

```
pvc 1/100 l2transport
 encapsulation aal0
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation default

To configure the default service instance on a port, use the **encapsulation default** command in the service instance mode. To delete the default service instance on a port, use the **no** form of this command.

encapsulation default

no encapsulation default

Syntax Description

This command has no arguments or keywords.

Command Default

No default service instance is configured on the port.

Command Modes

Service instance

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

If the default service instance is the only one configured on a port, the **encapsulation default** command matches all ingress frames on that port. If the default service instance is configured on a port that has other non-default service instances, the **encapsulation default** command matches frames that are unmatched by those non-default service instances (anything that does not meet the criteria of other services instances on the same physical interface falls into this service instance).

Only a single default service instance can be configured per interface. If you attempt to configure more than one default service instance per interface, the **encapsulation default** command is rejected.

Only one encapsulation command must be configured per service instance.

Examples

The following example shows how to configure a service instance on a port:

```
Router(config-if-srv)# encapsulation default
```

Related Commands

Command	Description
encapsulation dot1q (service instance)	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.

encapsulation dot1q (service instance)

To define the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **encapsulation dot1q** command in the service instance mode. To delete the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1q *vlan-id*[,*vlan-id*[-*vlain-id*]] [**native**]

no encapsulation dot1q *vlan-id*[,*vlan-id*[-*vlain-id*]] [**native**]

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. Optional) Comma must be entered to separate each VLAN ID range from the next range.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument.

Command Default

No matching criteria are defined.

Command Modes

Service instance

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The criteria for this command are: single VLAN, range of VLANs, and lists of the previous two.

A single 802.1Q service instance, allows one VLAN, multiple VLANs, or a range of VLANs. The native keyword can only be set if a single VLAN tag has been specified.

Only a single service instance per port is allowed to have the **native** keyword.

Only one encapsulation command may be configured per service instance.

Examples

The following example shows how to map 802.1Q frames ingress on an interface to the appropriate service instance:

```
Router(config-if-srv)# encapsulation dot1q 10
```

Related Commands

Command	Description
encapsulation default	Configures the default service instance on a port.
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.

encapsulation dot1q second-dot1q

To define the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance, use the **encapsulation dot1q second-dot1q** command in service instance mode. To delete the matching criteria to map Q-in-Q ingress frames on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}

no encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id*[,*vlan-id*[-*vlan-id*]]}

Syntax Description

vlan-id	VLAN ID, integer in the range 1 to 4094. Hyphen must be entered to separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs. (Optional) Comma must be entered to separate each VLAN ID range from the next range.
any	Any second tag in the range 1 to 4094.

Command Default

No matching criteria are defined.

Command Modes

Service instance

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The criteria for this command are: the outer tag must be unique and the inner tag may be a single VLAN, a range of VLANs or lists of the previous two.

QinQ service instance, allows single, multiple or range on second-dot1q.

Only one encapsulation command must be configured per service instance.

Examples

The following example shows how to map ingress frames to a service instance:

```
Router(config-if-srv)# encapsulation dot1q second-dot1q 20
```

Related Commands

Command	Description
encapsulation default	Configures the default service instance on a port.
encapsulation dot1q (service instance)	Defines the matching criteria to map 802.1Q frames ingress 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.

encapsulation frame-relay

To enable Frame Relay encapsulation, use the **encapsulation frame-relay** command in interface configuration mode. To disable Frame Relay encapsulation, use the **no** form of this command.

encapsulation frame-relay [**cisco** | **ietf**]

no encapsulation frame-relay [**ietf**]

Syntax Description

cisco	(Optional) Uses Cisco's own encapsulation, which is a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type.
ietf	(Optional) Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

Defaults

The default is Cisco's own encapsulation.

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

Use this command with no keywords to restore the default Cisco encapsulation, which is a 4-byte header with 2 bytes for the DLCI and 2 bytes to identify the packet type.

You should shut down the interface prior to changing encapsulation types. Although this is not required, shutting down the interface ensures that the interface is reset for the new encapsulation.

Examples

The following example configures Cisco Frame Relay encapsulation on interface serial 1:

```
interface serial 1
 encapsulation frame-relay
```

Use the **ietf** keyword if your router or access server is connected to another vendor's equipment across a Frame Relay network to conform with RFC 1490:

```
interface serial 1
 encapsulation frame-relay ietf
```

encapsulation frame-relay mfr

To create a multilink Frame Relay bundle link and to associate the link with a bundle, use the **encapsulation frame-relay mfr** command in interface configuration mode. To remove the bundle link from the bundle, use the **no** form of this command.

encapsulation frame-relay mfr *number* [*name*]

no encapsulation frame-relay mfr *number* [*name*]

Syntax Description

number	Interface number of the multilink Frame Relay bundle with which this bundle link will be associated.
name	(Optional) Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

Frame Relay encapsulation is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced on the Cisco 12000 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 *name* argument to assign a LID name to a bundle link. This name will be used to identify the bundle link to peer devices and to enable the devices to determine which bundle links are associated with which bundles. The LID name can also be assigned or changed by using the **frame-relay multilink lid** command on the bundle link interface. If the LID name is not assigned, the default name is the name of the physical interface.

Tip To minimize latency that results from the arrival order of packets, we recommend bundling physical links of the same line speed in one bundle.

To remove a bundle link from a bundle, use the **no encapsulation frame-relay mfr** command or configure a new type of encapsulation on the interface by using the **encapsulation** command.

Examples

The following example shows serial interface 0 being associated as a bundle link with bundle interface "mfr0." The bundle link identification name is "BL1."

```
interface mfr0
!
interface serial 0
 encapsulation frame-relay mfr0 BL1
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation	Sets the encapsulation method used by the interface.
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

encapsulation l2tpv3

To specify that Layer 2 Tunnel Protocol Version 3 (L2TPv3) is used as the data encapsulation method for tunneling IP traffic over the pseudowire, use the **encapsulation l2tpv3** command in pseudowire class or VC class configuration mode. To remove L2TPv3 as the encapsulation method, use the **no pseudowire-class** command (see the Usage Guidelines for more information).

encapsulation l2tpv3

no pseudowire-class

Syntax Description

This command has no arguments or keywords.

Command Default

No encapsulation method is specified.

Command Modes

Pseudowire class configuration
VC 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

This command must be configured if the pseudowire class will be referenced from an Xconnect configured to forward L2TPv3 traffic.

Once you specify the **encapsulation l2tpv3** command, you cannot remove it using the **no encapsulation l2tpv3** command. Nor can you change the command's setting using the **encapsulation mpls** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove the command, you must delete the pseudowire with the **no pseudowire-class** command. To change the type of encapsulation, remove the pseudowire with the **no pseudowire-class** command and re-establish the pseudowire and specify the new encapsulation type.

Examples

The following example shows how to configure L2TPv3 as the data encapsulation method for the pseudowire class named ether-pw:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation l2tpv3
```

The following example configures ATM AAL5 over L2TPv3 in VC class configuration mode:

```
vc-class atm aal5class
 encapsulation aal5
```

Related Commands

Command	Description
encapsulation mpls	Configures MPLS as the data encapsulation method over AToM-enabled IP/MPLS networks.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

encapsulation lapb

To exchange datagrams over a serial interface using Link Access Procedure, Balanced (LAPB) encapsulation, use the **encapsulation lapb** command in interface configuration mode.

encapsulation lapb [**dte** | **dce**] [**multi** | *protocol*]

Syntax Description

dte	(Optional) Specifies operation as a data terminal equipment (DTE) device. This is the default LAPB mode.
dce	(Optional) Specifies operation as a data communications equipment (DCE) device.
multi	(Optional) Specifies use of multiple LAN protocols to be carried on the LAPB line.
protocol	(Optional) A single protocol to be carried on the LAPB line. A single protocol can be one of the following: **appletalk**, **clns** (ISO CLNS), **decnet**, **ip**, and **ipx** (Novell IPX). IP is the default protocol.

Defaults

The default serial encapsulation is High-Level Data Link Control (HDLC). You must explicitly configure a LAPB encapsulation method.

DTE operation is the default LAPB mode. IP is the default protocol.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords and argument were introduced: **dte, dce, multi,** *protocol*.
12.2(13)T	The **apollo**, **vines**, and **xns** arguments were removed because support for Apollo Domain, Banyan VINES, and Xerox Network Systems is 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

LAPB encapsulations are appropriate only for private connections, where you have complete control over both ends of the link. Connections to X.25 networks should use an X.25 encapsulation configuration, which operates the X.25 Layer 3 protocol above a LAPB Layer 2.

One end of the link must be a logical DCE device, and the other end a logical DTE device. (This assignment is independent of the interface's hardware DTE or DCE identity.)

Both ends of the LAPB link must specify the same protocol encapsulation.

LAPB encapsulation is supported on serial lines configured for dial-on-demand routing (DDR). It can be configured on DDR synchronous serial and ISDN interfaces and on DDR dialer rotary groups. It is not supported on asynchronous dialer interfaces.

A single-protocol LAPB encapsulation exchanges datagrams of the given protocol, each in a separate LAPB information frame. You must configure the interface with the protocol-specific parameters needed—for example, a link that carries IP traffic will have an IP address defined for the interface.

A multiprotocol LAPB encapsulation can exchange any or all of the protocols allowed for a LAPB interface. It exchanges datagrams, each in a separate LAPB information frame. Two bytes of protocol identification data precede the protocol data. You need to configure the interface with all the protocol-specific parameters needed for each protocol carried.

Multiprotocol LAPB encapsulation supports transparent bridging. This feature requires use of the **encapsulation lapb multi** command followed by the **bridge-group** command, which identifies the bridge group associated with multiprotocol LAPB encapsulation. This feature does *not* support use of the **encapsulation lapb** *protocol* command with a **bridge** keyword.

LAPB encapsulation supports the priority and custom queueing features.

Examples

The following example sets the operating mode as DTE and specifies that AppleTalk protocol traffic will be carried on the LAPB line:

```
interface serial 1
 encapsulation lapb dte appletalk
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

encapsulation smds

To enable Switched Multimegabit Data Service (SMDS) on the desired interface, use the **encapsulation smds** interface configuration command.

encapsulation smds

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

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

The interface to which this command applies must be a serial interface. All subsequent SMDS configuration commands apply only to an interface with encapsulation SMDS.

Note The maximum packet size allowed in the SMDS specifications (TA-772) is 9188. This is larger than the packet size used by servers with most media. The Cisco default maximum transmission unit (MTU) size is 1500 bytes to be consistent with Ethernet. However, on the High Speed Serial Interface (HSSI), the default MTU size is 4470 bytes. If a larger MTU is used, the **mtu** command must be entered before the **encapsulation smds** command.

Caution The Cisco MCI card has buffer limitations that prevent setting the MTU size higher than 2048, and the HSSI card has buffer limitations that prevent setting the MTU size higher than 4500. Configuring higher settings can cause inconsistencies and performance problems.

Examples

The following example shows how to configure the SMDS service on serial interface 0:

```
interface serial 0
 encapsulation smds
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

encapsulation untagged

To define the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance, use the **encapsulation untagged** command in the service instance mode. To delete the matching criteria to map untagged ingress Ethernet frames on an interface to the appropriate service instance, use the **no** form of this command.

encapsulation untagged

no encapsulation untagged

Syntax Description

This command has no arguments or keywords.

Command Default

No matching criteria are defined.

Command Modes

Service instance mode

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Only one service instance per port is allowed to have untagged encapsulation. The reason is to be able to unambiguously map the incoming frames to the service instance. However, it is possible for a port that hosts an service instance matching untagged traffic to host other service instances that match tagged frames.

Only one encapsulation command may be configured per service instance.

Examples

The following example shows how to map untagged ingress Ethernet frames to a service instance:

```
Router(config-if-srv)# encapsulation untagged
```

Related Commands

Command	Description
encapsulation default	Configures the default service instance on a port.
encapsulation dot1q (service instance)	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 x25

To specify a serial interface's operation as an X.25 device, use the **encapsulation x25** command in interface configuration mode. To remove the specification, use the **no** form of this command.

encapsulation x25 [**dte** | **dce**] [**ddn** | **bfe** | **ietf**]

no encapsulation x25 [**dte** | **dce**] [**ddn** | **bfe** | **ietf**]

Syntax Description

dte	(Optional) Specifies operation as a data terminal equipment (DTE). This is the default X.25 mode.
dce	(Optional) Specifies operation as a data communications equipment (DCE).
ddn	(Optional) Specifies Defense Data Network (DDN) encapsulation on an interface using DDN X.25 Standard Service.
bfe	(Optional) Specifies Blacker Front End (BFE) encapsulation on an interface attached to a BFE device.
ietf	(Optional) Specifies that the interface's datagram encapsulation defaults to use of the Internet Engineering Task Force (IETF) standard method, as defined by RFC 1356.

Defaults

The default serial encapsulation is High-Level Data Link Control (HDLC). You must explicitly configure an X.25 encapsulation method.

DTE operation is the default X.25 mode. Cisco's traditional X.25 encapsulation method is the default.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added: • **dte** • **dce** • **ddn** • **bfe** • **ietf**
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

One end of an X.25 link must be a logical DCE device and the other end a logical DTE device. (This assignment is independent of the interface's hardware DTE or DCE identity.) Typically, when connecting to a public data network (PDN), the customer equipment acts as the DTE device and the PDN attachment acts as the DCE.

Cisco has long supported the encapsulation of a number of datagram protocols, using a standard means when available and a proprietary means when necessary. The IETF adopted a standard, RFC 1356, for encapsulating most types of datagram traffic over X.25. X.25 interfaces use Cisco's traditional method unless explicitly configured for IETF operation; if the **ietf** keyword is specified, that standard is used unless Cisco's traditional method is explicitly configured. For details see the **x25 map** command.

You can configure a router attaching to the DDN or to a BFE device to use their respective algorithms to convert between IP and X.121 addresses by using the **ddn** or **bfe** option, respectively. An IP address must be assigned to the interface, from which the algorithm will generate the interface's X.121 address. For proper operation, this X.121 address must not be modified.

A router DDN attachment can operate as either a DTE or a DCE device. A BFE attachment can operate only as a DTE device. The **ietf** option is not available if either the **ddn** or **bfe** option is selected.

Examples

The following example configures the interface for connection to a BFE device:

```
interface serial 0
 encapsulation x25 bfe
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.

ethernet evc

To define an Ethernet virtual connection (EVC) and to enter EVC configuration mode, use the **ethernet evc** command in global configuration mode. To delete the EVC, use the **no** form of this command.

ethernet evc *evc-id*

no ethernet evc *evc-id*

Syntax Description

evc-id	String from 1 to 100 characters that identifies the EVC.

Command Default

No EVCs are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

After you enter the **ethernet evc** command, the device enters EVC configuration mode and the following configuration commands are available:

- **default**—Sets the EVC to its default states.
- **exit**—Exits EVC configuration mode and returns the CLI to global configuration mode.
- **no**—Negates a command or returns a command to its default setting.
- **oam protocol**—Configures the Ethernet operations, administration, and maintenance (OAM) protocol and sets parameters.
- **uni count**—Configures a UNI count for the EVC.

Examples

The following example shows how to define an EVC named test1 and to enter EVC configuration mode:

```
Router(config)# ethernet evc test1
Router(config-evc)#
```

Related Commands

Command	Description
oam protocol	Configures the EVC OAM protocol.
service instance	Configures an Ethernet service instance and attaches an EVC to it.
show ethernet service evc	Displays information about configured EVCs.
uni count	Sets the UNI count for an EVC.

exp

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **exp** command in Frame Relay VC-bundle-member configuration mode. To remove the EXP level configuration from the PVC, use the **no** form of this command.

exp {*level* | **other**}

no exp

Syntax Description

level	The MPLS EXP level or levels for this Frame Relay PVC bundle member. The range is from 0 to 7. A PVC bundle member can be configured with a single level, multiple individual levels, a range of levels, multiple ranges of levels, or a combination of individual levels and level ranges. Levels can be specified in ascending or descending order (although a subsequent **show running-config** command will display them in ascending order). Examples are as follows: • 0 • 0,2,3 • 6-5 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining MPLS EXP levels that are not explicitly configured on any other bundle member PVCs.

Defaults

EXP levels are not configured.

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

Assignment of MPLS EXP levels to Frame Relay PVC bundle members lets you create differentiated services, because you can distribute the levels over the various PVC bundle members. You can map a single level or a range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different levels.

Use the **exp other** command to indicate that a PVC can carry traffic marked with EXP levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **exp other** command.

All EXP levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member but have no EXP level associated with it. As long as all valid EXP levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no EXP level configured will not participate in it.

The **exp** command is available only when MPLS is configured on the interface with the **mpls ip** command.

You can overwrite the EXP level configuration on a PVC by reentering the **exp** command with a new value.

The MPLS experimental bits are a bit-by-bit copy of the IP precedence bits. When Frame Relay PVC bundles are configured for IP precedence and MPLS is enabled, the **precedence** command is replaced by the **exp** command. When MPLS is disabled, the **exp** command is replaced by the **precedence** command.

Examples

The following example shows the configuration of four Frame Relay PVC bundle members in PVC bundle bundle1 configured with MPLS EXP level support:

```
interface serial 0.1 point-to-point
 encapsulation frame-relay
 ip address 10.1.1.1
 mpls ip
 frame-relay vc-bundle bundle1
 pvc 100 ny-control
 class control
 exp 7
 protect vc
 pvc 101 ny-premium
 class premium
 exp 6-5
 protect group
 no bump traffic
 bump explicit 7
 pvc 102 my-priority
 class priority
 exp 4-2
 protect group
 pvc 103 ny-basic
 class basic
 exp other
 protect group
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
mpls ip	Enables label switching of IPv4 packets on an interface.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
protect	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

fdl

To set the Facility Data Link (FDL) exchange standard for CSU controllers or to set the FDL exchange standard for a T1 interface that uses the Extended Super Frame (ESF) framing format, use the **fdl** command in interface configuration mode. To disable FDL support or to specify that there is no ESF FDL, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers

fdl {**att** | **ansi** | **all** | **none**}

no fdl {**att** | **ansi** | **all** | **none**}

Cisco 10000 Series Router

fdl {**att** | **ansi**}

no fdl {**att** | **ansi**}

Syntax Description

att	Specifies AT&T technical reference 54016 for ESF FDL exchange support.
ansi	Specifies ANSI T1.403 for ESF FDL exchange support.
all	Specifies both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.
none	Specifies that there is no support for ESF FDL exchange.

Defaults

ANSI T1.403 for ESF FDL exchange support

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)XK	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.0(5)T	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is available only for T1 links. This command sets the standard to be followed for FDL messaging through a 4-kbps out-of-band channel that a service provider uses to check for errors on the facility.

You must use the same FDL exchange standard as your service provider. If the setting is not correct, the link might not come up. You can configure a different standard on each T1 interface.

Note When using a multiport T1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, ESF framing and binary eight zero substitution (B8ZS) line encoding are supported. When using a multiport E1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, CRC4 multiframe framing and HDB3 line encoding are supported. These are the parameters specified by the ATM Forum, and they cannot be changed.

Examples

Cisco 2600 and Cisco 3600 Series Routers

The following example shows how to specify the ANSI standard and the AT&T standard for FDL exchange:

```
Router(config)# interface atm 0/2
Router(config-if)# fdl all
```

Cisco 10000 Series Router

The following example shows how to specify the AT&T standard for FDL exchange:

```
Router(config)# interface atm 1/0/0
Router(config-if)# fdl att
```

flow monitor type mace

To configure a Flexible NetFlow (FNF) flow monitor of type MACE and to enter Flexible NetFlow flow monitor configuration mode, use the **flow monitor type mace** command in global configuration mode. To remove the flow monitor for the Measurement, Aggregation, and Correlation Engine (MACE), use the **no** form of this command.

flow monitor type mace *name*

no flow monitor type mace *name*

Syntax Description

name	Name of the flow monitor.

Command Default

No flow monitor is configured for MACE.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **flow monitor type mace** command to define a set of metrics to be exported (flow record), the corresponding exporter information, and the cache timeout update. Use this command to configure a flow monitor for MACE and enter the FNF flow monitor configuration mode.

This mode accepts the following keywords:

- **cache**
- **default**
- **description**
- **exporter**
- **record**

Examples

The following example shows how to configure a flow monitor for MACE, mace1:

```
Router(config)# flow monitor type mace mace1
```

Related Commands

Command	Description
cache (Flexible NetFlow)	Configures a flow cache parameter for an FNF flow monitor.
default (Flexible NetFlow)	Configures the default values for an FNF flow exporter.

Command	Description
description (Flexible NetFlow)	Configures a description for an FNF flow sampler, flow monitor, flow exporter, or flow record.
exporter	Configures a flow exporter for an FNF flow monitor.
flow record	Creates or modifies an FNF flow record and enters FNF flow record configuration mode.

flow record type mace

To configure a flow record for the Measurement, Aggregation, and Correlation Engine (MACE) and to enter Flexible NetFlow flow record configuration mode, use the **flow record type mace** command in global configuration mode. To remove the flow record for MACE, use the **no** form of this command.

flow record type mace *name*

no flow record type mace *name*

Syntax Description

name	Name of the flow record.

Command Default

No flow record is configured for MACE.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **flow record type mace** command defines the key and non-key fields of MACE that are collected and exported. Use this command to configure a flow record for MACE and enter the FNF flow record configuration mode.

This mode accepts the following keywords:

- **collect**
- **default**
- **description**
- **execute**

Examples

The following example shows how to configure a flow record for MACE, mace1:

```
Router(config)# flow record type mace mace1
```

Related Commands

Command	Description
collect	Configures a flow cache parameter for an FNF flow monitor.
default (Flexible NetFlow)	Configures the default values for an FNF flow exporter.
description (Flexible NetFlow)	Configures a description for an FNF flow sampler, flow monitor, flow exporter, or flow record.

Command	Description
execute (Flexible NetFlow)	Executes a shell function for an FNF flow exporter.
flow record	Creates or modifies an FNF flow record and enters FNF flow record configuration mode.

frame-relay accounting adjust

To enable byte count adjustment at the permanent virtual circuit (PVC) level so that the number of bytes sent and received at the PVC corresponds to the actual number of bytes sent and received on the physical interface, use the **frame-relay accounting adjust** command in interface configuration mode. To disable byte count adjustment, use the **no** form of this command.

frame-relay accounting adjust

no frame-relay accounting adjust [**frf9**]

Syntax Description

frf9	(Optional) Payload compression using the Stacker method.

Note Use the **frf9** keyword only with the **no** form of this command.

Defaults

Byte count adjustment is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to return the number of bytes shown at the PVC level back to the number of bytes received at the PVC level without any adjustments. This command takes into consideration any dropped packets as well as compression and decompression that may occur after initial processing.

If you use the **no frame-relay accounting adjust frf9** command, then byte count includes dropped packets and traffic shaping, but not compression and decompression savings from FRF.9.

Examples

The following example enables Frame-Relay accounting adjustment:

```
Router# configure terminal
Router(config)# interface serial3/0
Router(config-if) frame-relay accounting adjust
```

The following example disables Frame-Relay accounting adjustment:

```
Router# configure terminal
Router(config)# interface serial3/0
Router(config-if) no frame-relay accounting adjust
Router(config-if)# end
```

The following example verifies that Frame-Relay accounting adjustment is disabled:

```
Router# show run interface serial3/0

Building configuration...

Current configuration :266 bytes
!
interface Serial3/0
 no ip address
 encapsulation frame-relay
 no frame-relay accounting adjust
end
```

Related Commands

Command	Description
show frame-relay pvc	Displays the total input and output bytes for a PVC and an interface as equal.

frame-relay adaptive-shaping

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay adaptive-shaping becn** and **frame-relay adaptive-shaping foresight** combinations of this command are hidden. Although these command combinations are still available in Cisco IOS software, the CLI interactive Help does not display them if you attempt to view them by entering a question mark at the command line.

These combinations of the command will be completely removed in a future release. For the **frame-relay adaptive-shaping becn** combination, this means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*. The **frame-relay adaptive-shaping foresight** combination of this command will not have a replacement command (or sequence of commands).

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay adaptive-shaping becn** combination of this command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*. The **frame-relay adaptive-shaping foresight** combination of this command does not have a replacement command (or sequence of commands).

To enable Frame Relay adaptive traffic shaping, use the **frame-relay adaptive-shaping** command in map-class configuration mode. To disable adaptive traffic shaping, use the **no** form of this command.

frame-relay adaptive-shaping {**becn** | **foresight** | **interface-congestion** [*queue-depth*]}

no frame-relay adaptive-shaping {**becn** | **foresight** | **interface-congestion**}

Syntax Description

becn	Enables rate adjustment in response to backward explicit congestion notification (BECN).
foresight	Enables rate adjustment in response to ForeSight messages.
interface-congestion	Enables rate adjustment in response to interface congestion.
queue-depth	(Optional) Maximum number of packets that can be in the interface queue before the interface is considered congested. The range is from 0 to 40 packets. The default is 0 packets.

Defaults

Frame Relay adaptive traffic shaping is not enabled.
Queue depth: 0 packets

Command Modes

Map-class configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(4)T	This command was modified to configure adaptive traffic shaping for interface congestion.
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.
Cisco IOS XE Release 2.6	This command was modified. The **frame-relay adaptive-shaping becn** and **frame-relay adaptive-shaping foresight** combinations of this command were hidden.
15.0(1)S	This command was modified. The **frame-relay adaptive-shaping becn** and **frame-relay adaptive-shaping foresight** combinations of this command were hidden.
15.1(3)T	This command was modified. The **frame-relay adaptive-shaping becn** and **frame-relay adaptive-shaping foresight** combinations of this command were hidden.
Cisco IOS XE Release 3.2S	This command was modified. The **frame-relay adaptive-shaping becn** combination of this command was replaced by an MQC command (or sequence of MQC commands). The **frame-relay adaptive-shaping foresight** combination was removed.

Usage Guidelines

This command replaces the **frame-relay becn-response-enable** command. If you use the **frame-relay becn-response-enable** command in scripts, you should replace it with the **frame-relay adaptive-shaping** command.

The **frame-relay adaptive-shaping** command configures a router to adjust virtual circuit (VC) sending rates in response to BECN or ForeSight backward congestion notification messages or interface congestion.

Include this command in a map-class definition and apply the map class either to the main interface or to a subinterface.

Adaptive traffic shaping for interface congestion can be configured along with BECN or ForeSight. When adaptive shaping for interface congestion is used with BECN or ForeSight, if interface congestion exceeds the queue depth, then the PVC send rate is reduced to minimum committed information rate (minCIR). When interface congestion drops below the queue depth, then the send rate is adjusted in response to BECN or ForeSight.

Note For adaptive traffic shaping for interface congestion to work, the sum of the minCIR values for all PVCs on the interface must be less than the usable interface bandwidth.

Examples

ForeSight: Example

This example shows the map-class definition for a router configured with traffic shaping and Router ForeSight enabled:

```
interface Serial0
 no ip address
 encapsulation frame-relay
```

```
 frame-relay traffic-shaping
 frame-relay class control-A
!
map-class frame-relay control-A
 frame-relay adaptive-shaping foresight
 frame-relay cir 56000
 frame-relay bc 64000
```

Adaptive Shaping for Interface Congestion: Example

In the following example, the queue depth is set at 10 packets. If the number of packets in the interface queue exceeds 10, the rate of traffic destined for PVC 200 will be reduced to the minCIR. When the number of packets in the interface queue drops below 10, then the traffic rate will immediately return to the CIR.

```
interface serial0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 200
 class adjust_vc_class_rate
!
map-class frame-relay adjust_vc_class_rate
 frame-relay cir 64000
 frame-relay mincir 32000
 frame-relay adaptive-shaping interface-congestion 10
```

Related Commands

Command	Description
frame-relay traffic-shaping	Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay address registration auto-address

To enable a router to automatically select a management IP address for Enhanced Local Management Interface (ELMI) address registration, use the **frame-relay address registration auto-address** command in global configuration mode. To disable automatic address selection, use the **no** form of this command.

frame-relay address registration auto-address

no frame-relay address registration auto-address

Syntax Description

This command has no arguments or keywords.

Defaults

Auto address selection is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)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

During system initialization, if no management IP address is configured, then the router automatically selects the IP address of one of the interfaces. The router will choose an Ethernet interface first and then serial and other interfaces. If you do not want the router to select a management IP address during system initialization, you can store the **no** form of this command in the configuration.

When automatic address selection is disabled and an IP address has not been configured using the **frame-relay address registration ip** global configuration command, the IP address for ELMI address registration will be set to 0.0.0.0.

The **no frame-relay address registration ip** command will set the IP address to 0.0.0.0, even when Frame Relay automatic address selection is enabled.

If you configure the IP address using the **frame-relay address registration ip** global configuration command, the IP address you configure will overwrite the IP address chosen automatically by the router.

If you enable automatic address selection after configuring the IP address using the **frame-relay address registration ip** global configuration command, the IP address chosen automatically by the router will overwrite the IP address you originally configured.

Examples

The following example shows ELMI enabled on serial interface 0. The automatic IP address selection mechanism is disabled, and no other management IP address has been configured, so the device will share a valid ifIndex and a management IP address of 0.0.0.0.

```
interface Serial 0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay qos-autosense
!
no frame-relay address registration auto-address
```

Related Commands

Command	Description
frame-relay address-reg enable	Enables ELMI address registration on an interface.
frame-relay address registration ip	Configures the IP address to be used for ELMI address registration.
frame-relay qos-autosense	Enables ELMI on the Cisco router.

frame-relay address registration ip

To configure the IP address for Enhanced Local Management Interface (ELMI) address registration, use the **frame-relay address registration ip** command in global configuration mode. To set the IP address to 0.0.0.0, use the **no** form of this command.

frame-relay address registration ip *address*

no frame-relay address registration ip

Syntax Description

address	IP address to be used for ELMI address registration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)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

A management IP address configured by using the **frame-relay address registration ip** command will overwrite the IP address chosen by the router when automatic address selection is enabled.

The **no frame-relay address registration ip** command will disable automatic IP address selection and set the management IP address to 0.0.0.0.

If you enable automatic address selection with the **frame-relay address registration auto-address** global command after configuring the IP address using the **frame-relay address registration ip** global configuration command, the IP address chosen automatically by the router will overwrite the IP address you originally configured.

Examples

The following example shows ELMI enabled on serial interface 0. The IP address to be used for ELMI address registration is configured, so automatic IP address selection is disabled by default.

```
interface Serial 0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay qos-autosense
!
frame-relay address registration ip address 10.1.1.1
```

Related Commands

Command	Description
frame-relay address-reg enable	Enables ELMI address registration on an interface.
frame-relay address registration auto-address	Enables a router to automatically select the IP address to be used for ELMI address registration.
frame-relay qos-autosense	Enables ELMI on a Cisco router.

frame-relay address-reg enable

To enable Enhanced Local Management Interface (ELMI) address registration on an interface, use the **frame-relay address-reg enable** command in interface configuration mode. To disable ELMI address registration, use the **no** form of this command.

frame-relay address-reg enable

no frame-relay address-reg enable

Syntax Description

This command has no arguments or keywords.

Defaults

ELMI address registration is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)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

ELMI address registration is enabled by default when ELMI is enabled.

Examples

The following example shows ELMI address registration disabled on serial interface 0.

```
interface Serial 0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay qos-autosense
 no frame-relay address-reg enable
```

Related Commands

Command	Description
frame-relay address registration auto-address	Enables a router to automatically select the IP address to be used for ELMI address registration.
frame-relay address registration ip	Configures the IP address to be used for ELMI address registration.
frame-relay qos-autosense	Enables ELMI on a Cisco router.

frame-relay bc

Note Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.0(1)S, the **frame-relay bc** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay bc** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To specify the incoming or outgoing committed burst size (Bc) for a Frame Relay virtual circuit, use the **frame-relay bc** command in map-class configuration mode. To reset the committed burst size to the default, use the **no** form of this command.

frame-relay bc {**in** | **out**} *bits*

no frame-relay bc {**in** | **out**} *bits*

Syntax Description

in | **out**	Incoming or outgoing; if neither is specified, both in and out values are set.
bits	Committed burst size, in bits. Range is from 300 to 16000000. Default is 7000.

Defaults

7000 bits

Command Modes

Map-class configuration

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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.

Release	Modification
15.0(1)S	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The Frame Relay committed burst size is specified within a map class to request a certain burst rate for the circuit. Although it is specified in bits, an implicit time factor is the sampling interval *Tc* on the switch, which is defined as the burst size divided by the committed information rate (CIR).

Examples

In the following example, the serial interface already has a basic configuration, and a map group called "group1" has already been defined. The example shows a map-list configuration that defines the source and destination addresses for bermuda, provides IP and IPX addresses, and ties the map list definition to the map class called "class1". Then traffic-shaping parameters are defined for the map class.

```
map-list group1 local-addr X121 31383040703500 dest-addr X121 31383040709000
 ip 172.21.177.26 class class1 ietf
 ipx 123.0000.0c07.d530 class class1 ietf

map-class frame-relay class1
 frame-relay cir in 2000000
 frame-relay mincir in 1000000
 frame-relay cir out 15000
 frame-relay mincir out 10000
 frame-relay bc in 15000
 frame-relay bc out 9600
 frame-relay be in 10000
 frame-relay be out 10000
 frame-relay idle-timer 30
```

Related Commands

Command	Description
frame-relay be	Sets the incoming or outgoing excess burst size (Be) for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.

frame-relay be

Note Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.0(1)S, the **frame-relay be** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay be** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To set the incoming or outgoing excess burst size (Be) for a Frame Relay virtual circuit, use the **frame-relay be** command in map-class configuration mode. To reset the excess burst size to the default, use the **no** form of this command.

frame-relay be {**in** | **out**} *bits*

no frame-relay be {**in** | **out**} *bits*

Syntax Description

in	Incoming.
out	Outgoing.
bits	Excess burst size, in bits.

Defaults

7000 bits

Command Modes

Map-class configuration

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.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The Frame Relay excess burst size is specified within a map class to request a certain burst rate for the circuit. Although it is specified in bits, an implicit time factor is the sampling interval *Tc* on the switch, which is defined as the burst size divided by the committed information rate (CIR).

Examples

In the following example, the serial interface already has a basic configuration, and a map group called "bermuda" has already been defined. The example shows a map-list configuration that defines the source and destination addresses for bermuda, provides IP and IPX addresses, and ties the map list definition to the map class called "jamaica". Then traffic-shaping parameters are defined for the map class.

```
map-list bermuda local-addr X121 31383040703500 dest-addr X121 31383040709000
 ip 172.21.177.26 class jamaica ietf
 ipx 123.0000.0c07.d530 class jamaica ietf

map-class frame-relay jamaica
 frame-relay cir in 2000000
 frame-relay mincir in 1000000
 frame-relay cir out 15000
 frame-relay mincir out 10000
 frame-relay bc in 15000
 frame-relay bc out 9600
 frame-relay be in 10000
 frame-relay be out 10000
 frame-relay idle-timer 30
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing committed burst size (Bc) for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.

frame-relay broadcast-queue

To create a special queue for a specified interface to hold broadcast traffic that has been replicated for transmission on multiple data-link connection identifiers (DLCIs), use the **frame-relay broadcast-queue** command in interface configuration mode.

frame-relay broadcast-queue *size byte-rate packet-rate*

Syntax Description

size	Number of packets to hold in the broadcast queue.
byte-rate	Maximum number of bytes to be sent per second.
packet-rate	Maximum number of packets to be sent per second.

Defaults

size: 64 packets
byte-rate: 256000 bytes per second
packet-rate: 36 packets per second

Command Modes

Interface 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

For purposes of the Frame Relay broadcast queue, *broadcast traffic* is defined as packets that have been replicated for transmission on multiple DLCIs. However, the broadcast traffic does not include the original routing packet or service access point (SAP) packet, which passes through the normal queue. Because of timing sensitivity, bridged broadcasts and spanning-tree packets are also sent through the normal queue. The Frame Relay broadcast queue is managed independently of the normal interface queue. It has its own buffers and a configurable service rate.

A broadcast queue is given a maximum transmission rate (throughput) limit measured in bytes per second and packets per second. The queue is serviced to ensure that only this maximum is provided. The broadcast queue has priority when transmitting at a rate below the configured maximum, and hence has a guaranteed minimum bandwidth allocation. The two transmission rate limits are intended to avoid flooding the interface with broadcasts. The actual limit in any second is the first rate limit that is reached.

Given the transmission rate restriction, additional buffering is required to store broadcast packets. The broadcast queue is configurable to store large numbers of broadcast packets.

The queue size should be set to avoid loss of broadcast routing update packets. The exact size will depend on the protocol being used and the number of packets required for each update. To be safe, set the queue size so that one complete routing update from each protocol and for each DLCI can be stored. As a general rule, start with 20 packets per DLCI. Typically, the byte rate should be less than both of the following:

- *N/4* times the minimum remote access rate (measured in *bytes* per second), where *N* is the number of DLCIs to which the broadcast must be replicated.
- 1/4 the local access rate (measured in *bytes* per second).

The packet rate is not critical if you set the byte rate conservatively. Set the packet rate at 250-byte packets.

Examples

The following example specifies a broadcast queue to hold 80 packets, to have a maximum byte transmission rate of 240000 bytes per second, and to have a maximum packet transmission rate of 160 packets per second:

```
frame-relay broadcast-queue 80 240000 160
```

frame-relay cir

Note Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.0(1)S, the **frame-relay cir** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay cir** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To specify the incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit, use the **frame-relay cir** command in map-class configuration mode. To reset the CIR to the default, use the **no** form of this command.

frame-relay cir {**in** | **out**} *bps*

no frame-relay cir {**in** | **out**} *bps*

Syntax Description

in	Specifies an incoming CIR.
out	Specifies an outgoing CIR.
bps	CIR in bits per second.

Defaults

56000 bits per second

Command Modes

Map-class configuration

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.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

Use this command to specify a CIR for an SVC. The specified CIR value is sent through the SETUP message to the switch, which then attempts to provision network resources to support this value.

Examples

The following example sets a higher committed information rate for incoming traffic than for outgoing traffic (which is going out on a slow WAN line):

```
frame-relay cir in 2000000
frame-relay cir out 9600
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing committed burst size (Bc) for a Frame Relay VC.
frame-relay be	Sets the incoming or outgoing excess burst size (Be) for a Frame Relay VC.

frame-relay class

To associate a map class with an interface or subinterface, use the **frame-relay class** command in interface configuration mode. To remove the association between the interface or subinterface and the named map class, use the **no** form of this command.

frame-relay class *name*

no frame-relay class *name*

Syntax Description

name	Name of the map class to associate with this interface or subinterface.

Defaults

No map class is defined.

Command Modes

Interface configuration

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

This command can apply to interfaces or subinterfaces.

All relevant parameters defined in the *name* map class are inherited by each virtual circuit created on the interface or subinterface. For each virtual circuit, the precedence rules are as follows:

1. Use the map class associated with the virtual circuit if it exists.
2. If not, use the map class associated with the subinterface if the map class exists.
3. If not, use map class associated with interface if the map class exists.
4. If not, use the interface default parameters.

Examples

The following example associates the slow_vcs map class with the serial 0.1 subinterface and defines the slow_vcs map class to have an outbound CIR value of 9600:

```
interface serial 0.1
 frame-relay class slow_vcs

map-class frame-relay slow_vcs
 frame-relay cir out 9600
```

If a virtual circuit exists on the serial 0.1 interface and is associated with some other map class, the parameter values of the second map class override those defined in the slow_vc map class for that virtual circuit.

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay congestion threshold de

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay congestion threshold de** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay congestion threshold de** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To configure the threshold at which discard-eligible (DE)-marked packets will be discarded from the traffic-shaping queue of a switched permanent virtual circuit (PVC), use the **frame-relay congestion threshold de** command in map-class configuration mode. To reconfigure the threshold, use the **no** form of this command.

frame-relay congestion threshold de *percentage*

no frame-relay congestion threshold de *percentage*

Syntax Description

percentage	Threshold at which DE-marked packets will be discarded, specified as a percentage of the maximum queue size.

Defaults

100%

Command Modes

Map-class 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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.

Release	Modification
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The **frame-relay congestion threshold de** command applies only to default FIFO traffic-shaping queues.

You must enable Frame Relay switching using the **frame-relay switching** global command before Frame Relay congestion management parameters will be effective on switched PVCs.

Examples

The following example illustrates the configuration of the DE congestion threshold in the Frame Relay map class called “perpvc_congestion”:

```
map-class frame-relay perpvc_congestion
 frame-relay congestion threshold de 50
```

Related Commands

Command	Description
frame-relay congestion-management	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
frame-relay congestion threshold ecn	Configures the threshold at which ECN bits are set on packets in the traffic-shaping queue of a switched PVC.
threshold de	Configures the threshold at which DE-marked packets are discarded from switched PVCs on the output interface.
threshold ecn	Configures the threshold at which ECN bits are set on packets in switched PVCs on the output interface.

frame-relay congestion threshold ecn

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay congestion threshold ecn** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay congestion threshold ecn** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To configure the threshold at which explicit congestion notice (ECN) bits will be set on packets in the traffic-shaping queue of a switched permanent virtual circuit (PVC), use the **frame-relay congestion threshold ecn** command in map-class configuration mode. To reconfigure the threshold, use the **no** form of this command.

frame-relay congestion threshold ecn *percentage*

no frame-relay congestion threshold ecn *percentage*

Syntax Description

percentage	Threshold at which ECN bits will be set on packets, specified as a percentage of the maximum queue size.

Defaults

100%

Command Modes

Map-class 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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.

Release	Modification
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

The **frame-relay congestion threshold ecn** command applies only to default FIFO traffic-shaping queues.

One ECN threshold applies to all traffic on a traffic-shaping queue. You cannot configure separate thresholds for committed and excess traffic.

You must enable Frame Relay switching using the **frame-relay switching** global command before the **frame-relay congestion threshold ecn** command will be effective on switched PVCs.

Examples

The following example illustrates the configuration of the ECN congestion threshold in the Frame Relay map class called “perpvc_congestion”:

```
map-class frame-relay perpvc_congestion
 frame-relay congestion threshold ecn 50
```

Related Commands

Command	Description
frame-relay congestion-management	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
frame-relay congestion threshold de	Configures the threshold at which DE-marked packets are discarded from the traffic-shaping queue of a switched PVC.
threshold de	Configures the threshold at which DE-marked packets are discarded from switched PVCs on the output interface.
threshold ecn	Configures the threshold at which ECN bits are set on packets in switched PVCs on the output interface.

frame-relay congestion-management

To enable Frame Relay congestion management functions on all switched permanent virtual circuits (PVCs) on an interface, and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** command in interface configuration mode. To disable Frame Relay congestion management, use the **no** form of this command.

frame-relay congestion-management

no frame-relay congestion-management

Syntax Description

This command has no arguments or keywords.

Defaults

Frame Relay congestion management is not enabled on switched PVCs.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(27)SXA	This command was integrated into Cisco IOS Release 12.2(27)SXA.
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.

Usage Guidelines

You must enable Frame Relay switching, using the **frame-relay switching** global command, before you can configure Frame Relay congestion management.

Frame Relay congestion management is supported only when the interface is configured with class-based weighted fair queuing (WFQ).

Examples

In the following example, the **frame-relay congestion-management** command enables Frame Relay congestion management on serial interface 1. The command also enters Frame Relay congestion management configuration mode so that congestion threshold parameters can be configured.

```
interface serial1
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay congestion-management
  threshold ecn be 0
  threshold ecn bc 20
```

Related Commands

Command	Description
threshold ecn	Configures the threshold at which ECN bits are set on packets in switched PVCs on the output interface.

frame-relay custom-queue-list

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay custom-queue-list** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay custom-queue-list** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To specify a custom queue to be used for the virtual circuit queueing associated with a specified map class, use the **frame-relay custom-queue-list** command in map-class configuration mode. To remove the specified queueing from the virtual circuit and cause it to revert to the default first-come, first-served queueing, use the **no** form of this command.

frame-relay custom-queue-list *list-number*

no frame-relay custom-queue-list *list-number*

Syntax Description

list-number	Custom queue list number.

Defaults

If this command is not entered, the default queueing is first come, first served.

Command Modes

Map-class configuration

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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.

Release	Modification
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

Use the **queue-list** commands to define the custom queue.

Only one form of queueing can be associated with a particular map class; subsequent definitions overwrite previous ones.

Examples

The following example configures a custom queue list for the “fast_vcs” map class:

```
map-class frame-relay fast_vcs
 frame-relay custom-queue-list 1

queue-list 1 queue 4 byte-count 100
```

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay de-group

To specify the discard eligibility (DE) group number to be used for a specified data-link connection identifier (DLCI), use the **frame-relay de-group** command in interface configuration mode. To disable a previously defined group number assigned to a specified DLCI, use the **no** form of this command with the relevant keyword and arguments.

frame-relay de-group *group-number dlci*

no frame-relay de-group [*group-number*] [*dlci*]

Syntax Description

group-number	DE group number to apply to the specified DLCI number, from 1 to 10.
dlci	DLCI number.

Defaults

No DE group is defined.

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

To disable all previously defined group numbers, use the **no** form of this command with no arguments.

This command requires that Frame Relay be enabled.

Frame Relay DE group functionality is supported on process-switched packets only.

The DE bit is not set or recognized by the Frame Relay switching code, but must be recognized and interpreted by the Frame Relay network.

Note Frame Relay DE group functionality is being replaced by the Modular QoS CLI (MQC) DE marking functionality. For information about the MQC commands that are used to configure Frame Relay DE marking, refer to the *Cisco IOS Quality of Service Configuration Guide* and *Cisco IOS Quality of Service Command Reference*.

Examples

The following example specifies that group number 3 will be used for DLCI 170:

```
frame-relay de-group 3 170
```

Related Commands

Command	Description
frame-relay de-list	Defines a DE list specifying the packets that have the DE bit set and thus are eligible for discarding during congestion on the Frame Relay switch.

frame-relay de-list

To define a discard eligibility (DE) list specifying the packets that have the DE bit set and thus are eligible for discarding when congestion occurs on the Frame Relay switch, use the **frame-relay de-list** command in global configuration mode. To delete a portion of a previously defined DE list, use the **no** form of this command.

frame-relay de-list *list-number* {**protocol** *protocol* | **interface** *type number*} *characteristic*

no frame-relay de-list *list-number* {**protocol** *protocol* | **interface** *type number*} *characteristic*

Syntax Description

list-number	Number of the DE list.
protocol *protocol*	One of the following values corresponding to a supported protocol or device: **arp**—Address Resolution Protocol. **appletalk**—AppleTalk. **bridge**—bridging device. **clns**—ISO Connectionless Network Service. **clns_es**—CLNS end systems. **clns_is**—CLNS intermediate systems. **compressedtcp**—Compressed TCP. **decnet**—DECnet. **decnet_node**—DECnet end node. **decnet_router-L1**—DECnet Level 1 (intra-area) router. **decnet_router-L2**—DECnet Level 2 (interarea) router. **ip**—Internet Protocol. **ipx**—Novell Internet Packet Exchange Protocol.
interface *type*	One of the following interface types: **serial**, **null**, or **ethernet**.
number	Interface number.
characteristic	One of the following values: **fragments**—Fragmented IP packets **gt** *bytes*—Sets the DE bit for packets larger than the specified number of bytes (including the 4-byte Frame Relay encapsulation). **list** *access-list-number*—Previously defined access list number. **lt** *bytes*—Sets the DE bit for packets smaller than the specified number of bytes (including the 4-byte Frame Relay encapsulation). **tcp** *port*—TCP packets to or from a specified port. **udp** *port*—User Datagram Protocol (UDP) packets to or from a specified port.

Defaults

Discard eligibility is not defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **apollo**, **vines**, and **xns** arguments were removed because Apollo Domain, 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

To remove an entire DE list, use the **no** form of this command with no options and arguments.

This prioritizing feature requires that the Frame Relay network be able to interpret the DE bit as indicating which packets can be dropped first in case of congestion, or which packets are less time sensitive, or both.

When you calculate packet size, include the data packet size, the ICMP header, the IP header, and the Frame Relay encapsulation bytes. For example, count 92 bytes of data, 8 bytes for the ICMP header, 20 bytes for the IP header, and 4 bytes for the Frame Relay encapsulation, which equals 124 bytes.

Examples

The following example specifies that IP packets larger than 512 bytes (including the 4-byte Frame Relay encapsulation) will have the DE bit set:

```
frame-relay de-list 1 protocol ip gt 512
```

frame-relay end-to-end keepalive error-threshold

To modify the keepalive error threshold value, use the **frame-relay end-to-end keepalive error-threshold** command in map-class configuration mode. To reset the error threshold value to its default, use the **no** form of this command.

frame-relay end-to-end keepalive error-threshold {**send** | **receive**} *count*

no frame-relay end-to-end keepalive error-threshold {**send** | **receive**}

Syntax Description

send	Number of send-side errors in the event window before keepalive status goes from up to down.
receive	Number of receive-side errors in the event window before keepalive status goes from up to down.
count	Number of errors required. The maximum value is 32.

Defaults

The default value for both the send and receive error threshold is 2.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(5)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

The send-side value can be configured only in bidirectional and request modes. The receive-side value can be configured only in bidirectional and reply modes. See the **frame-relay end-to-end keepalive mode** command. When you configure the error threshold, also configure the event window. See the **frame-relay end-to-end keepalive event-window** command.

Examples

The following example shows increasing the receive-side error threshold to 4 and changing the event window to 7:

```
map-class frame-relay olga
  frame-relay end-to-end keepalive reply
  frame-relay end-to-end keepalive error-threshold receive 4
  frame-relay end-to-end keepalive event-window receive 7
```

Related Commands

Command	Description
frame-relay end-to-end keepalive event-window	Modifies the keepalive event window value.
frame-relay end-to-end keepalive mode	Enables Frame Relay end-to-end keepalives.
frame-relay end-to-end keepalive success-events	Modifies the keepalive success events value.
frame-relay end-to-end keepalive timer	Modifies the keepalive timer.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
show frame-relay end-to-end keepalive	Displays statistics about Frame Relay end-to-end keepalive.

frame-relay end-to-end keepalive event-window

To modify the keepalive event window value, use the **frame-relay end-to-end keepalive event-window** command in map-class configuration mode. To reset the event window size to the default, use the **no** form of this command.

frame-relay end-to-end keepalive event-window {**send** | **receive**} *size*

no frame-relay end-to-end keepalive event-window {**send** | **receive**}

Syntax Description

send	Send-side event window for which size is being configured.
receive	Receive-side event window for which size is being configured.
size	Number of events in the event window. The maximum value is 32.

Defaults

The default value for both the send and receive event windows is 3.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(5)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

The send-side value can be configured only in bidirectional and request modes. The receive-side value can be configured only in bidirectional and reply modes. See the **frame-relay end-to-end keepalive mode** command. When you configure the event window, also configure the error-threshold. See the **frame-relay end-to-end keepalive error-threshold** command.

Examples

The following example shows increasing the receive-side error threshold to 4 and changing the event window to 7:

```
map-class frame-relay olga
 frame-relay end-to-end keepalive reply
 frame-relay end-to-end keepalive error-threshold receive 4
 frame-relay end-to-end keepalive event-window receive 7
```

Related Commands

Command	Description
frame-relay end-to-end keepalive error-threshold	Modifies the keepalive error threshold value.
frame-relay end-to-end keepalive mode	Enables Frame Relay end-to-end keepalives.
frame-relay end-to-end keepalive success-events	Modifies the keepalive success events value.
frame-relay end-to-end keepalive timer	Modifies the keepalive timer.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
show frame-relay end-to-end keepalive	Displays statistics about Frame Relay end-to-end keepalive.

frame-relay end-to-end keepalive mode

To enable Frame Relay end-to-end keepalives, use the **frame-relay end-to-end keepalive mode** command in map-class configuration mode. To disable Frame Relay end-to-end keepalives, use the **no** form of this command.

frame-relay end-to-end keepalive mode {**bidirectional** | **request** | **reply** | **passive-reply**}

no frame-relay end-to-end keepalive mode

Syntax Description

bidirectional	Enables bidirectional mode.
request	Enables request mode.
reply	Enables reply mode.
passive-reply	Enables passive reply mode.

Defaults

When a Frame Relay end-to-end keepalive mode is enabled, default values depend on which mode is selected. For the meaning of the parameters, see the **frame-relay end-to-end keepalive timer**, **frame-relay end-to-end keepalive event-window**, **frame-relay end-to-end keepalive error-threshold**, and **frame-relay end-to-end keepalive success-events** commands.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(5)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

In bidirectional mode, both ends of a virtual circuit (VC) send keepalive requests and respond to keepalive requests. If one end of the VC is configured in the bidirectional mode, the other end must also be configured in the bidirectional mode.

In request mode, the router sends keepalive requests and expects replies from the other end of the VC. If one end of a VC is configured in the request mode, the other end must be configured in the reply or passive-reply mode.

In reply mode, the router does not send keepalive requests, but waits for keepalive requests from the other end of the VC and replies to them. If no keepalive request has arrived within the timer interval, the router times out and increments the error counter by 1. If one end of a VC is configured in the reply mode, the other end must be configured in the request mode.

In passive-reply mode, the router does not send keepalive requests, but waits for keepalive requests from the other end of the VC and replies to them. No timer is set when in this mode, and the error counter is not incremented. If one end of a VC is configured in the passive-reply mode, the other end must be configured in the request mode.

Table 13 displays parameter values for send and receive sides in bidirectional mode.

Table 13 Bidirectional Mode

Parameter	Send-Side	Receive-Side
Timer	10 seconds	15 seconds
Event window	3	3
Error threshold	2	2
Success events	2	2

Table 14 displays parameter values for send- and receive-sides in request mode.

Table 14 Request Mode

Parameter	Send-Side	Receive-Side
Timer	10 seconds	no value set
Event window	3	no value set
Error threshold	2	no value set
Success events	2	no value set

Table 15 displays parameter values for send- and receive-sides in reply mode.

Table 15 Reply Mode

Parameter	Send-Side	Receive-Side
Timer	no value set	15 seconds
Event window	no value set	3
Error threshold	no value set	2
Success events	no value set	2

Passive-Reply Mode

In passive-reply mode, no values are set.

Examples

The following example configures one end of a VC to send keepalive requests and respond to keepalive requests from the other end of the VC:

```
map-class frame-relay vcgrp1
 frame-relay end-to-end keepalive bidirectional
```

The following example configures one end of a VC to reply to keepalive requests and to increment its error counter if no keepalive requests are received 30 seconds after the latest request:

```
map-class frame-relay oro34
 frame-relay end-to-end keepalive reply
 frame-relay end-to-end keepalive timer receive 30
```

Related Commands

Command	Description
frame-relay end-to-end keepalive error-threshold	Modifies the keepalive error threshold value.
frame-relay end-to-end keepalive event-window	Modifies the keepalive event window value.
frame-relay end-to-end keepalive success-events	Modifies the keepalive success events value.
frame-relay end-to-end keepalive timer	Modifies the keepalive timer.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
show frame-relay end-to-end keepalive	Displays statistics about Frame Relay end-to-end keepalive.

frame-relay end-to-end keepalive success-events

To modify the keepalive success events value, use the **frame-relay end-to-end keepalive success-events** command in map-class configuration mode. To reset the success events value to its default, use the **no** form of this command.

frame-relay end-to-end keepalive success-events {**send** | **receive**} *count*

no frame-relay end-to-end keepalive success-events {**send** | **receive**}

Syntax Description

send	The number of consecutive send-side success events required to change the keepalive state from down to up.
receive	The number of consecutive receive-side success events required to change the keepalive state from down to up.
count	Number of consecutive success events required. The maximum value is 32.

Defaults

The default value for both the send and receive success events is 2.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(5)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

The send-side value can be configured only in bidirectional and request modes. The receive-side value can be configured only in the bidirectional and reply modes. See the **frame-relay end-to-end keepalive mode** command.

If the success events value is set low at the same time that a low value is set for the error threshold value of the **frame-relay end-to-end keepalive error-threshold** command, the keepalive state of the VC may flap from state to state.

Examples

The following example shows how to increase the success events value:

```
map-class frame-relay vcgrp4
 frame-relay end-to-end keepalive request
 frame-relay end-to-end keepalive success-events send 4
```

Related Commands

Command	Description
frame-relay end-to-end keepalive error-threshold	Modifies the keepalive error threshold value.
frame-relay end-to-end keepalive event-window	Modifies the keepalive event window value.
frame-relay end-to-end keepalive mode	Enables Frame Relay end-to-end keepalives.
frame-relay end-to-end keepalive timer	Modifies the keepalive timer.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
show frame-relay end-to-end keepalive	Displays statistics about Frame Relay end-to-end keepalive.

frame-relay end-to-end keepalive timer

To modify the keepalive timer value, use the **frame-relay end-to-end keepalive timer** command in map-class configuration mode. To reset the timer value to its default, use the **no** form of this command.

frame-relay end-to-end keepalive timer {**send** | **receive**} *number*

no frame-relay end-to-end keepalive timer {**send** | **receive**}

Syntax Description

send	How frequently to send a keepalive request.
receive	How long before the receive-side error counter is incremented if no request is received.
number	Number, in seconds, for the timer to expire.

Defaults

Send timer: 10 seconds
Receive timer: 15 seconds

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(5)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

The send-side value can be configured only in bidirectional and request modes. The receive-side value can be configured only in the bidirectional and reply modes. See the **frame-relay end-to-end keepalive mode** command.

The send-side timer expires if a reply has not been received *number* seconds after a request is sent. The receive-side timer expires if a request has not been received *number* seconds after the previous request.

Examples

The following example shows how to set up one end of a virtual circuit (VC) to send a keepalive request every 15 seconds and increment the error counter if more than 22 seconds elapse between receiving keepalive responses:

```
map-class frame-relay vcgrp1
 frame-relay end-to-end keepalive bidirectional
 frame-relay end-to-end keepalive timer send 15
 frame-relay end-to-end keepalive timer receive 22
```

Related Commands

Command	Description
frame-relay end-to-end keepalive error-threshold	Modifies the keepalive error threshold value.
frame-relay end-to-end keepalive event-window	Modifies the keepalive event window value.
frame-relay end-to-end keepalive mode	Enables Frame Relay end-to-end keepalives.
frame-relay end-to-end keepalive success-events	Modifies the keepalive success events value.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
show frame-relay end-to-end keepalive	Displays statistics about Frame Relay end-to-end keepalive.

frame-relay fair-queue

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay fair-queue** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay fair-queue** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To enable weighted fair queueing for one or more Frame Relay permanent virtual circuits (PVCs), use the **frame-relay fair-queue** command in map-class configuration mode. To disable weighted fair queueing for a Frame Relay map class, use the **no** form of this command.

frame-relay fair-queue [*congestive-discard-threshold* [*number-dynamic-conversation-queues* [*number-reservable-conversation-queues* [*max-buffer-size-for-fair-queues*]]]]

no frame-relay fair-queue [*congestive-discard-threshold* [*number-dynamic-conversation-queues* [*number-reservable-conversation-queues* [*max-buffer-size-for-fair-queues*]]]]

Syntax Description

congestive-discard-threshold	(Optional) Specifies the number of messages allowed in each queue. The range is from 1 to 4096 messages; the default is 64.
number-dynamic-conversation- queues	(Optional) Specifies the number of dynamic queues to be used for best-effort conversations—normal conversations not requiring any special network services. Valid values are 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096; the default is 16.
number-reservable-conversation-queues	(Optional) Specifies the number of reserved queues to be used for carrying voice traffic. The range is from 0 to 100; the default is 0. (The command-line interface (CLI) will not allow a value of less than 2 if fragmentation is configured for the Frame Relay map-class.)
max-buffer-size-for-fair-queues	(Optional) Specifies the maximum buffer size in bytes for all of the fair queues. The range is from 0 to 4096 bytes; the default is 600.

Defaults

Weighted fair queueing is not enabled.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

To use this command, you must first associate a Frame Relay map class with a specific data-link connection identifier (DLCI), and then enter map-class configuration mode and enable or disable weighted fair queueing for that map class.

When Frame Relay fragmentation is enabled, weighted fair queueing is the only queueing strategy allowed.

If this command is entered without any accompanying numbers, the default values for each of the four parameters will be set. If you desire to alter only the value of the first parameter (*congestive_discard_threshold*), you only need to enter the desired value for that parameter. If you desire to alter only the value of the second, third, or fourth parameters, you must enter values for the preceding parameters as well as for the parameter you wish to change.

Examples

The following example shows how to enable weighted fair queueing and set the default parameter values for the "vofr" Frame Relay map class on a Cisco 2600 series, 3600 series, or 7200 series router or on a Cisco MC3810:

```
interface serial 1/1
 frame-relay interface-dlci 100
  class vofr
  exit
map-class frame-relay vofr
 frame-relay fair-queue
```

The following example shows how to enable weighted fair queueing and set the *congestive_discard_threshold* parameter to a value other than the default value for the "vofr" Frame Relay map class on a Cisco 2600 series, 3600 series, or 7200 series router or on an MC3810 concentrator:

```
interface serial 1/1
 frame-relay interface-dlci 100
```

```
  class vofr
  exit
map-class frame-relay vofr
 frame-relay fair-queue 255
```

The following example shows how to enable weighted fair queueing and set the *number_reservable_conversation_queues* to a value of 25 for the "vofr" Frame Relay map class on a Cisco 2600 series, 3600 series, or 7200 series router or on a Cisco MC3810:

```
interface serial 1/1
 frame-relay interface-dlci 100
  class vofr
  exit
map-class frame-relay vofr
 frame-relay fair-queue 64 256 25
```

Related Commands

Command	Description
class (virtual circuit)	Associates a map class with a specified DLCI.
frame-relay fragment	Enables fragmentation for a Frame Relay map class.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay fecn-adapt

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay fecn-adapt** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay fecn-adapt** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To enable Frame Relay traffic-shaping reflection of forward explicit congestion notifications (FECNs) as backward explicit congestion notifications (BECNs), use the **frame-relay fecn-adapt** command in map-class configuration mode. To disable this reflection, use the **no** form of this command.

frame-relay fecn-adapt

no frame-relay fecn-adapt

Syntax Description

This command has no arguments or keywords.

Command Default

Frame Relay traffic-shaping reflection of FECNs as BECNs is disabled.

Command Modes

Map-class configuration (config-map-class)

Command History

Release	Modification
12.2(11)T	This command was introduced in a release earlier than Cisco IOS Release 12.2(11)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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Examples

The following example shows how to configure the **frame-relay fecn-adapt** command:

```
Router> enable
Router# configure terminal
Router(config)# map-class frame-relay class1
Router(config-map-class)# frame-relay fecn-adapt
Router(config-map-class)# end
```

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define values for PVCs and SVCs.

frame-relay fragment

To enable fragmentation of Frame Relay frames for a Frame Relay map class, use the **frame-relay fragment** command in map-class configuration mode. To disable Frame Relay fragmentation, use the **no** form of this command.

frame-relay fragment *fragment-size* [**switched**]

no frame-relay fragment

Syntax Description

fragment-size	Specifies the number of payload bytes from the original Frame Relay frame that will go into each fragment. This number excludes the Frame Relay header of the original frame. All the fragments of a Frame Relay frame except the last will have a payload size equal to *fragment-size*; the last fragment will have a payload less than or equal to *fragment-size*. Valid values are from 16 to 1600; the default is 53.
switched	(Optional) Specifies that fragmentation will be enabled on a switched permanent virtual circuit (PVC).

Command Default

Fragmentation is disabled.

Command Modes

Map-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(23)SX	This command was integrated into Cisco IOS Release 12.0(23)SX.
12.1(2)T	Support of end-to-end FRF.12 fragmentation was extended to switched Frame Relay PVCs.
12.1(2)E	This command was integrated into Cisco IOS Release 12.1(2)E.
12.1(5)T	This command was implemented on Cisco 7500 series routers with a Versatile Interface Processor.
12.2(27)SBB	This command was integrated into Cisco IOS Release 12.2(27)SBB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Usage Guidelines

You should enable fragmentation for low-speed links (meaning those operating at less than 768 kbps).

Frame Relay fragmentation is enabled on a per-PVC basis. Before enabling Frame Relay fragmentation, you must first associate a Frame Relay map class with a specific data-link connection identifier (DLCI) and then enter map-class configuration mode and enable or disable fragmentation for that map class. In addition, you must enable Frame Relay traffic shaping on the interface.

Selecting a Fragmentation Format

Frame Relay frames are fragmented using one of the following formats, depending on how the PVC is configured:

- Pure end-to-end FRF.12
- FRF.11 Annex C
- Cisco proprietary

Only pure end-to-end FRF.12 fragmentation can be configured on switched PVCs.

Cisco recommends pure end-to-end FRF.12 fragmentation on PVCs that are carrying VoIP packets and on PVCs that share the link with other PVCs carrying Voice over Frame Relay (VoFR) traffic.

In pure end-to-end FRF.12 fragmentation, Frame Relay frames having a payload less than the fragment size configured for that PVC are transmitted without the fragmentation header.

FRF.11 Annex C fragmentation and Cisco proprietary fragmentation are used when VoFR frames are transmitted on a PVC. When fragmentation is enabled on a PVC, and when command **vofr** is configured on that PVC, FRF.11 Annex C format is implemented. When command **vofr cisco** is configured, Cisco proprietary format is implemented.

In FRF.11 Annex C and Cisco proprietary fragmentation, VoFR frames are never fragmented, and all data packets (including VoIP packets) contain the fragmentation header regardless of the payload size.

Selecting a Fragment Size

You should set the fragment size based on the lowest port speed between the routers. For example, for a hub-and-spoke Frame Relay topology where the hub has a T1 speed and the remote routers have 64-kbps port speeds, the fragmentation size must be set for the 64-kbps speed on both routers. Any other PVCs that share the same physical interface must use the same fragmentation size used by the voice PVC.

With pure end-to-end FRF.12 fragmentation, you should select a fragment size that is larger than the voice packet size.

Table 16 shows the recommended fragmentation sizes for a serialization delay of 10 ms.

Table 16 Recommended Fragment Size for 10-ms Serialization Delay

Lowest Link Speed in Path	Recommended Fragment Size
56 kbps	70 bytes
64 kbps	80 bytes
128 kbps	160 bytes
256 kbps	320 bytes
512 kbps	640 bytes
768 kbps	1000 bytes
1536 kbps	1600 bytes

Examples

FRF.12 Fragmentation on a Switched PVC: Example

The following example shows how to configure pure end-to-end FRF.12 fragmentation in a map class that is named data. The map class is associated with switched PVC 20 on serial interface 3/3:

```
Router(config)# frame-relay switching

Router(config)# interface Serial3/2
```

```
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay intf-type dce
Router(config-if)# exit

Router(config)# interface Serial3/3
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay traffic-shaping
Router(config-if)# frame-relay interface-dlci 20 switched
Router(config-fr-dlci)# class data
Router(config-fr-dlci)# exit
Router(config-if)# frame-relay intf-type dce
Router(config-if)# exit

Router(config)# map-class frame-relay data
Router(config-map-class)# frame-relay fragment 80 switched
Router(config-map-class)# frame-relay cir 64000
Router(config-map-class)# frame-relay bc 640
Router(config-map-class)# exit

Router(config)# connect data Serial3/2 16 Serial3/3 20
```

End-to-End FRF.12 Fragmentation: Example

The following example shows how to enable pure end-to-end FRF.12 fragmentation for a map class. named frag. The fragment payload size is set to 40 bytes. Frame Relay traffic shaping is required on the PVC; the only queueing type supported on the PVC when fragmentation is configured is weighted fair queueing (WFQ).

```
Router(config)# interface serial 1/0/0
Router(config-if)# frame-relay traffic-shaping
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay cir 128000
Router(config-map-class)# frame-relay bc 1280
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# frame-relay fair-queue
Router(config-map-class)# exit
```

The following example is for the same configuration on a VIP-enabled Cisco 7500 series router:

```
Router(config)# class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)# exit
Router(config)# policy-map llq
Router(config-pmap)# class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)# service-policy llq
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface serial 1/0/0.1
Router(config-if)# frame-relay interface-dlci 100
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
```

```
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
Router(config-map-class)# exit
```

FRF.11 Annex C Fragmentation Configuration: Example

The following example shows how to enable FRF.11 Annex C fragmentation for data on a Cisco MC3810 PVC configured for VoFR. Fragmentation must be configured if a VoFR PVC will carry data. The fragment payload size is set to 40 bytes. Frame Relay traffic shaping is required on the PVC; the only queueing type supported on the PVC when fragmentation is configured is weighted fair queueing (WFQ):

```
Router(config)# interface serial 1/1
Router(config-if)# frame-relay traffic-shaping
Router(config-if)# frame-relay interface-dlci 101
Router(config-fr-dlci)# vofr
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay cir 128000
Router(config-map-class)# frame-relay bc 1280
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# frame-relay fair-queue
Router(config-map-class)# exit
```

The following example is for the same configuration on a VIP-enabled Cisco 7500 series router:

```
Router(config)# class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)# exit
Router(config)# policy-map llq
Router(config-pmap)# class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)# service-policy llq
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial 1/1/0.1
Router(config-if)# frame-relay interface-dlci 101
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
Router(config-map-class)# exit
```

Cisco-Proprietary Fragmentation: Example

The following example shows how to enable Cisco-proprietary Frame Relay fragmentation for a Frame Relay map class named frag on a Cisco 2600 series, Cisco 3600 series, or Cisco 7200 series router, starting from global configuration mode. The fragment payload size is set to 40 bytes. Frame Relay traffic shaping is required on the PVC; the only queueing type supported on the PVC when fragmentation is configured is weighted fair queueing (WFQ):

```
Router(config)# interface serial 2/0/0
Router(config-if)# frame-relay traffic-shaping
Router(config-if)# frame-relay interface-dlci 102
```

```
Router(config-fr-dlci)# vofr cisco
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay cir 128000
Router(config-map-class)# frame-relay bc 1280
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# frame-relay fair-queue
```

The following example is for the same configuration on a VIP-enabled Cisco 7500 series router:

```
Router(config)# class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)# exit
Router(config)# policy-map llq
Router(config-pmap)# class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)# service-policy llq
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface serial 2/0/0.1
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# class frag
Router(config-fr-dlci)# exit

Router(config)# map-class frame-relay frag
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
```

Related Commands

Command	Description
class (virtual circuit)	Associates a map class with a specified DLCI.
debug frame-relay fragment	Displays information related to Frame Relay fragmentation on a PVC.
frame-relay fair-queue	Enables weighted fair queueing for one or more Frame Relay PVCs.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay traffic-shaping	Enables traffic shaping and per-virtual circuit queueing for all PVCs and SVCs on a Frame Relay interface.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
vofr	Enables Voice over Frame Relay (VoFR) on a specific data-link connection identifier (DLCI) and configuration of specific subchannels on that DLCI.

frame-relay fragment end-to-end

To enable fragmentation of Frame Relay frames on an interface, use the **frame-relay fragment end-to-end** command in interface configuration mode. To disable Frame Relay fragmentation on an interface, use the **no** form of this command.

frame-relay fragment *fragment-size* **end-to-end**

no frame-relay fragment end-to-end

Syntax Description

fragment-size	Specifies the number of payload bytes from the original Frame Relay frame that will go into each fragment. This number excludes the Frame Relay header of the original frame. Valid values are from 16 to 1600 bytes; the default is 53.

Command Default

Fragmentation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Interface fragmentation and class-based fragmentation cannot be configured at the same time. To configure class-based fragmentation that can be applied to individual permanent virtual circuits (PVCs), use the **frame-relay fragment** command in map-class configuration mode.

Interface fragmentation supports the following fragment formats:

- End-to-end FRF.12
- FRF.11 Annex C
- Cisco proprietary

When fragmentation is enabled on an interface, all PVCs on the main interface and its subinterfaces will have fragmentation enabled with the same configured fragment size.

All the fragments of a Frame Relay frame except the last fragment will have a payload size equal to *fragment-size*; the last fragment will have a payload less than or equal to *fragment-size*.

When configuring fragmentation on an interface that has low-latency queueing, configure the fragment size to be greater than the largest high-priority frame that is expected. This configuration prevents higher-priority traffic from being fragmented and queued behind lower-priority fragmented frames. If the size of a high-priority frame is larger than the configured fragment size, the high-priority frame is fragmented.

Local Management Interface (LMI) traffic is fragmented.

Interface fragmentation and Frame Relay traffic shaping cannot be configured at the same time.

Examples

The following example shows the configuration of low-latency queueing, FRF.12 fragmentation, and shaping on serial interface 3/2. Traffic from the priority queue will not be interleaved with fragments from the class-default queue, because shaping is configured.

```
class-map voice
 match access-group 101

policy-map llq
 class voice
  priority 64

policy-map shaper
 class class-default
  shape average 96000
  service-policy llq

interface serial 3/2
 ip address 10.0.0.1 255.0.0.0
 encapsulation frame-relay
 bandwidth 128
 clock rate 128000
 service-policy output shaper
 frame-relay fragment 80 end-to-end

access-list 101 match ip any host 10.0.0.2
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, or specifies the default class before you configure its policy.
debug frame-relay fragment	Displays information related to Frame Relay fragmentation on a PVC.
frame-relay fragment	Enables fragmentation of Frame Relay frames for a Frame Relay map class.

frame-relay fragmentation voice-adaptive

To enable voice-adaptive Frame Relay fragmentation, use the **frame-relay fragmentation voice-adaptive** command in interface configuration mode. To disable voice-adaptive Frame Relay fragmentation, use the **no** form of this command.

frame-relay fragmentation voice-adaptive [**deactivation** *seconds*]

no frame-relay fragmentation voice-adaptive

Syntax Description

deactivation *seconds*	(Optional) Number of seconds that must elapse after the last voice packet is transmitted before fragmentation is deactivated. The range is from 1 to 10000.

Defaults

Voice-adaptive Frame Relay fragmentation is not enabled.
Seconds: 30

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Frame Relay voice-adaptive fragmentation can be used in conjunction with Frame Relay voice-adaptive traffic shaping to reduce network congestion and improve voice transmission quality.

The **frame-relay fragmentation voice-adaptive** command can be used only on main interfaces. This command is not supported on subinterfaces.

Frame Relay voice-adaptive fragmentation enables a router to fragment large packets whenever packets (usually voice) are detected in the low latency queueing priority queue or H.323 call setup signaling packets are present. When there are no packets in the priority queue for a configured period of time and signaling packets are not present, fragmentation is stopped.

Note Although the priority queue is generally used for voice traffic, Frame Relay voice-adaptive fragmentation will respond to any packets (voice or data) in the priority queue.

Note the following prerequisites for Frame Relay voice-adaptive fragmentation:

- End-to-end fragmentation must be configured in a map class by using the **frame-relay fragment** command or on the interface by using the **frame-relay fragment end-to-end** command.
- Frame Relay traffic shaping or traffic shaping using the Modular QoS CLI (MQC) must be configured. If end-to-end fragmentation is configured on the interface, traffic shaping using the MQC must be configured.
- Low latency queueing must be configured.

Frame Relay voice-adaptive fragmentation supports FRF.12 fragmentation only. Neither FRF.11 Annex C nor Cisco proprietary fragmentation is supported.

Examples

The following examples show the configuration of Frame Relay voice-adaptive traffic shaping and fragmentation. The first example shows end-to-end fragmentation configured in a map class that is associated with PVC 100. In the second example, end-to-end fragmentation is configured directly on the interface.

With both example configurations, priority-queue packets or H.323 call setup signaling packets destined for PVC 100 will result in the reduction of the sending rate from the committed information rate (CIR) to the minimum CIR and the activation of FRF.12 end-to-end fragmentation. If signaling packets and priority-queue packets are not detected for 50 seconds, the sending rate will increase to CIR and fragmentation will be deactivated.

Frame Relay Voice-Adaptive Fragmentation with End-to-End Fragmentation Configured in a Map Class: Example

```
interface serial0
 encapsulation frame-relay
 frame-relay fragmentation voice-adaptive deactivation 50
 frame-relay interface-dlci 100
  class voice_adaptive_class
!
map-class frame-relay voice_adaptive_class
 frame-relay fair-queue
 frame-relay fragment 80
 service-policy output shape
```

Frame Relay Voice-Adaptive Fragmentation with End-to-End Fragmentation Configured on the Interface: Example

```
interface serial0
 encapsulation frame-relay
 frame-relay fragmentation voice-adaptive deactivation 50
 frame-relay fragment 80 end-to-end
 frame-relay interface-dlci 100
  class voice_adaptive_class
```

Related Commands

Command	Description
frame-relay fragment	Enables fragmentation of Frame Relay frames for a Frame Relay map class.
frame-relay fragment end-to-end	Enables fragmentation of Frame Relay frames on an interface.
shape fr-voice-adapt	Enables Frame Relay voice-adaptive traffic shaping.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

frame-relay holdq

To configure the maximum size of a traffic-shaping queue on a switched permanent virtual circuit (PVC), use the **frame-relay holdq** command in map-class configuration mode. To reconfigure the size of the queue, use the **no** form of this command.

frame-relay holdq *queue-size*

no frame-relay holdq *queue-size*

Syntax Description

queue-size	Size of the traffic-shaping queue, as specified in maximum number of packets. The range is from 1 to 2048.

Defaults

40 packets for FIFO and 600 packets for CBWFQ

Command Modes

Map-class configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(4)T	This command was modified to allow configuration of the maximum buffers in CBWFQ traffic shaping queues (as enabled by the **service-policy output** map-class command).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(6)T7	The maximum allowable value for *queue-size* was increased to 2048.
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

You must enable Frame Relay traffic shaping, using the **frame-relay traffic-shaping** interface command, before **frame-relay holdq** and other traffic-shaping map-class commands will be effective.

You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **frame-relay holdq** command will be effective on switched PVCs.

The **frame-relay holdq** command can be applied to switched PVCs that use FIFO default queueing.

Examples

The following example illustrates the configuration of the maximum size of the traffic-shaping queue on a switched PVC. The queue size is configured in a map class called “perpvc_congestion”:

```
map-class frame-relay perpvc_congestion
 frame-relay holdq 100
```

Related Commands

Command	Description
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
frame-relay traffic-shaping	Enables both traffic shaping and per-PVC queueing for all PVCs and SVCs on a Frame Relay interface.

frame-relay idle-timer

To specify the idle timeout interval for a switched virtual circuit (SVC), use the **frame-relay idle-timer** command in map-class configuration mode. To reset the idle timer to its default interval, use the **no** form of this command.

frame-relay idle-timer [**in** | **out**] *seconds*

no frame-relay idle-timer *seconds*

Syntax Description

in	(Optional) timeout interval applies to inbound packet activity.
out	(Optional) timeout interval applies to outbound packet activity.
seconds	Time interval, in seconds, with no frames exchanged on a switched virtual circuit, after which the SVC is released.

Defaults

120 seconds

Command Modes

Map-class configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3	The following keywords were added: • **in** • **out**
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 **frame-relay idle-timer** command applies to switched virtual circuits that are associated with the map class where the idle-timer is defined.

The idle timer must be tuned for each application. Routing protocols such as Routing Information Protocol (RIP) might keep the SVC up indefinitely because updates go out every 10 seconds.

Beginning in Cisco IOS Release 11.3, if **in** and **out** are not specified in the command, the timeout interval applies to both timers. In Cisco IOS Release 11.2, the timeout interval applies to the outbound timer.

Examples

The following example defines the traffic rate and idle timer for the fast_vcs map class and applies those values to DLCI 100, which is associated with that map class:

```
interface serial 0
 frame-relay interface-dlci 100
  class fast_vc

map-class frame-relay fast_vcs
 frame-relay traffic-rate 56000 128000
 frame-relay idle-timer 30
```

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay ifmib-counter64

To enable 64-bit interface counter support on Frame Relay interfaces and subinterfaces that have a line speed of less than 20 Mbps, use the **frame-relay ifmib-counter64** command in interface configuration mode. To disable 64-bit counter support on Frame Relay interfaces and subinterfaces that have a line speed of less than 20 Mbps, use the **no** form of this command.

frame-relay ifmib-counter64 [**if** | **subif**]

no frame-relay ifmib-counter64 [**if** | **subif**]

Syntax Description

if	(Optional) Enables 64-bit interface counters for Frame Relay interfaces and subinterfaces.
subif	(Optional) Enables 64-bit interface counters for Frame Relay subinterfaces only.

Command Default

64-bit interface counters are not supported for interfaces that have a line speed of less than 20 Mbps.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.3(10)	This command was integrated into Cisco IOS Release 12.3(10).
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Entering the **frame-relay ifmib-counter64** command with no keyword produces the same result as entering the **frame-relay ifmib-counter64** command with the **if** keyword.

Examples

The following example shows how to enable support for 64-bit interface counters on serial interface 5/3 and associated subinterfaces:

```
interface Serial 5/3
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 load-interval 30
 no keepalive
 frame-relay ifmib-counter64
```

Related Commands

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

frame-relay interface-dlci

To assign a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, to assign a specific permanent virtual circuit (PVC) to a DLCI, or to apply a virtual template configuration for a PPP session, use the **frame-relay interface-dlci** command in interface configuration mode. To remove this assignment, use the **no** form of this command.

frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

no frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

BOOTP Server Only

frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

no frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

Syntax Description

dlci	DLCI number to be used on the specified subinterface.
ietf	(Optional) Specifies Internet Engineering Task Force (IETF) as the type of Frame Relay encapsulation.
cisco	(Optional) Specifies Cisco encapsulation as the type of Frame Relay encapsulation.
voice-cir *cir*	(Optional; supported on the Cisco MC3810 only.) Specifies the upper limit on the voice bandwidth that may be reserved for this DLCI. The default is the committed information rate (CIR) configured for the Frame Relay map class. For more information, see the "Usage Guidelines" section.
ppp	(Optional) Enables the circuit to use the PPP in Frame Relay encapsulation.
virtual-template-name	(Optional) Name of the virtual template interface to apply the PPP connection to.
protocol ip *ip-address*	(Optional) Indicates the IP address of the main interface of a new router or access server onto which a router configuration file is to be automatically installed over a Frame Relay network. Use this option only when this device will act as the BOOTP server for automatic installation over Frame Relay.

Command Default

No DLCI is assigned.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
11.3(1)MA	The **voice-encap** option was added for the Cisco MC3810.
12.0(1)T	The **ppp** keyword and *virtual-template-name* argument were added.
12.0(2)T	The **voice-cir** option was added for the Cisco MC3810.
12.0(3)T	The **x25 profile** keyword was added.
12.0(4)T	Usage guidelines for the Cisco MC3810 were added.
12.0(7)XK	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
12.1(2)T	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command is typically used for subinterfaces; however, it can also be used on main interfaces. Using the **frame-relay interface-dlci** command on main interfaces will enable the use of routing protocols on interfaces that use Inverse ARP. The **frame-relay interface-dlci** command on a main interface is also valuable for assigning a specific class to a single PVC where special characteristics are desired. Subinterfaces are logical interfaces associated with a physical interface. You must specify the interface and subinterface before you can use this command to assign any DLCIs and any encapsulation or broadcast options.

A DLCI cannot be configured on a subinterface if the same DLCI has already been configured on the main interface. If the same DLCI is to be configured on the subinterface as on the main interface, the DLCI on the main interface must be removed first before it is configured on the subinterface. The DLCI on the main interface can be removed by using the **no frame-relay interface-dlci** command on the main interface.

This command is required for all point-to-point subinterfaces; it is also required for multipoint subinterfaces for which dynamic address resolution is enabled. It is not required for multipoint subinterfaces configured with static address mappings.

Use the **protocol ip** *ip-address* option only when this router or access server will act as the BOOTP server for auto installation over Frame Relay.

By issuing the **frame-relay interface-dlci** interface configuration command, you enter Frame Relay DLCI interface configuration mode (see the first example below). This gives you the following command options, which must be used with the relevant class or X.25-profile names you previously assigned:

- **class** *name*—Assigns a map class to a DLCI.
- **default**—Sets a command to its defaults.
- **no** {**class** *name* | **x25-profile** *name*}—Cancels the relevant class or X.25 profile.
- **x25-profile** *name*—Assigns an X.25 profile to a DLCI. (Annex G.)

A Frame Relay DLCI configured for Annex G can be thought of as a single logical X.25/LAPB interface. Therefore, any number of X.25 routes may be configured to route X.25 calls to that logical interface.

The **voice-cir** option on the Cisco MC3810 provides call admission control; it does not provide traffic shaping. A call setup will be refused if the unallocated bandwidth available at the time of the request is not at least equal to the value of the **voice-cir** option.

When configuring the **voice-cir** option on the Cisco MC3810 for Voice over Frame Relay, do not set the value of this option to be higher than the physical link speed. If Frame Relay traffic shaping is enabled for a PVC that is sharing voice and data, do not configure the **voice-cir** option to be higher than the value set with the **frame-relay mincir** command.

Note On the Cisco MC3810 only, the **voice-cir** option performs the same function as the **frame-relay voice bandwidth** map-class configuration command introduced in Cisco IOS Release 12.0(3)XG.

Examples

The following example assigns DLCI 100 to serial subinterface 5.17:

```
! Enter interface configuration and begin assignments on interface serial 5.
interface serial 5
! Enter subinterface configuration by assigning subinterface 17.
interface serial 5.17
! Now assign a DLCI number to subinterface 5.17.
frame-relay interface-dlci 100
```

The following example specifies DLCI 26 over serial subinterface 1.1 and assigns the characteristics under virtual-template 2 to this PPP connection:

```
Router(config)# interface serial1.1 point-to-point
Router(config-if)# frame-relay interface-dlci 26 ppp virtual-template2
```

The following example shows an Annex G connection being created by assigning the X.25 profile "NetworkNodeA" to Frame Relay DLCI interface 20 on serial interface 1 (having enabled Frame Relay encapsulation on that interface):

```
Router(config)# interface serial 1
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 20
Router(config-fr-dlci)# x25-profile NetworkNodeA
```

The following example assigns DLCI 100 to serial subinterface 5.17:

```
Router(config)# interface serial 5
Router(config-if)# interface serial 5.17
Router(config-if)# frame-relay interface-dlci 100
```

The following example assigns DLCI 80 to the main interface first and then removes it before assigning the same DLCI to the subinterface. The DLCI must be removed from the main interface first, because the same dlci cannot be assigned to the subinterface after already being assigned to the main interface:

```
Router(config)# interface serial 2/0
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 80
Router(config-fr-dlci)# exit
Router(config-if)# interface serial 2/0
Router(config-if)# no frame-relay interface-dlci 80
Router(config-if)# interface serial 2/0.1
Router(config-subif)# frame-relay interface-dlci 80
```

Related Commands

Command	Description
frame-relay class	Associates a map class with an interface or subinterface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interface	Displays P1024B/C information.
vofr	Configures subchannels and enables Voice over Frame Relay for a specific DLCI.

frame-relay interface-dlci switched

To indicate that a Frame Relay data-link connection identifier (DLCI) is switched, use the **frame-relay interface-dlci switched** command in interface configuration mode. To remove this assignment, use the **no** form of this command.

frame-relay interface-dlci *dlci* **switched**

no frame-relay interface-dlci *dlci* **switched**

Syntax Description

dlci	DLCI number to be used on the specified interface or subinterface.

Defaults

No DLCI is assigned.
The default PVC type is terminated.

Command Modes

Interface 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 **frame-relay interface-dlci switched** command to allow a map class to be associated with a switched permanent virtual circuit (PVC).

You cannot change an existing PVC from terminated to switched or vice versa. You must delete the PVC and recreate it in order to change the type.

Use the **frame-relay interface-dlci switched** command to create switched PVCs for configuring Frame Relay-ATM network interworking (FRF.5) and Frame Relay-ATM service interworking (FRF.8).

By issuing the **frame-relay interface-dlci switched** interface configuration command, you enter Frame Relay DLCI interface configuration mode (see the example below).

Examples

In the following example, DLCI 16 on serial interface 0 is identified as a switched PVC and is associated with a map class called shape256K.

```
Router(config) # interface serial0
Router(config-if) # encapsulation frame-relay
Router(config-if) # frame-relay interface-dlci 16 switched
Router(config-fr-dlci) # class shape256K
```

Related Commands

Command	Description
connect (Frame Relay)	Defines connections between Frame Relay PVCs.
frame-relay class	Associates a map class with an interface or subinterface.
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

frame-relay intf-type

To configure a Frame Relay switch type, use the **frame-relay intf-type** command in interface configuration mode. To disable the switch, use the **no** form of this command.

frame-relay intf-type [**dce** | **dte** | **nni**]

no frame-relay intf-type [**dce** | **dte** | **nni**]

Syntax Description

dce	(Optional) Router or access server functions as a switch connected to a router.
dte	(Optional) Router or access server is connected to a Frame Relay network.
nni	(Optional) Router or access server functions as a switch connected to a switch—supports Network-to-Network Interface (NNI) connections.

Defaults

The router or access server is connected to a Frame Relay network.

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

This command can be used only if Frame Relay switching has previously been enabled globally by means of the **frame-relay switching** command.

Examples

The following example configures a DTE switch type:

```
frame-relay switching
!
interface serial 2
 frame-relay intf-type dte
```

frame-relay inverse-arp

To reenable Inverse Address Resolution Protocol (Inverse ARP) on a specified interface, subinterface, data-link connection identifier (DLCI), or Frame Relay permanent virtual circuit (PVC) bundle if Inverse ARP was previously disabled, use the **frame-relay inverse-arp** command in interface configuration mode. To disable Inverse ARP, use the **no** form of this command.

frame-relay inverse-arp [*protocol*] [*dlci* | **vc-bundle** *vc-bundle-name*]

no frame-relay inverse-arp [*protocol*] [*dlci* | **vc-bundle** *vc-bundle-name*]

Syntax Description

protocol	(Optional) One of the following values: **appletalk**, **decnet**, **ip**, and **ipx**.
dlci	(Optional) One of the DLCI numbers used on the interface. Acceptable values are integers from 16 through 1007, inclusive.
vc-bundle *vc-bundle-name*	(Optional) A specific Frame Relay PVC bundle configured on the interface.

Defaults

Inverse ARP is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **vc-bundle** *vc-bundle-name* keyword and argument pair was added. The **apollo**, **vines**, and **xns** keywords were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer available in the Cisco IOS software.
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.

Usage Guidelines

To enable Inverse ARP for all protocols that were enabled before the prior **no frame-relay inverse-arp** command was issued, use the **frame-relay inverse-arp** command without arguments. To disable Inverse ARP for all protocols supported on an interface, use the **no frame-relay inverse-arp** command without arguments.

To enable or disable Inverse ARP for a specific protocol and DLCI pair, use both the *protocol* and *dlci* arguments. To enable or disable Inverse ARP for a specific protocol and Frame Relay PVC bundle (consisting of up to eight DLCIs), use both the *protocol* and **vc-bundle** *vc-bundle-name* elements.

To enable or disable Inverse ARP for all protocols on a DLCI or Frame Relay PVC bundle, use either the *dlci* argument by itself or the **vc-bundle** *vc-bundle-name* keyword and argument pair by itself. To enable or disable Inverse ARP for a specific protocol for all DLCIs on the specified interface or subinterface, use only the *protocol* argument.

When a Frame Relay PVC bundle is specified, only one member of the PVC bundle will handle Inverse ARP packets. By default, the bundle member PVC that handles precedence or EXP level 6 or DSCP level 63 handles Inverse ARP packets. Use the **inarp** command to configure a different PVC bundle member to handle Inverse ARP packets.

This implementation of Inverse ARP is based on RFC 1293. It allows a router or access server running Frame Relay to discover the protocol address at the other side of a virtual circuit.

The **show frame-relay map** command displays the word “dynamic” to flag virtual circuits that are created dynamically by Inverse ARP.

Examples

The following example sets Inverse ARP on DLCI 100 on an interface running IPX:

```
interface serial 0
 frame-relay inverse-arp ipx 100
```

Related Commands

Command	Description
clear frame-relay-inarp	Clears dynamically created Frame Relay maps, which are created by the use of Inverse ARP.
inarp	Specifies the PVC bundle member used to handle the Inverse ARP packets.
show frame-relay map	Displays the current map entries and information about the connections.

frame-relay ip tcp compression-connections

To specify the maximum number of TCP header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip tcp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

frame-relay ip tcp compression-connections *number*

no frame-relay ip tcp compression-connections

Syntax Description

number	Maximum number of TCP header compression connections. The range is from 3 to 256.

Command Default

256 header compression connections

Command Modes

Interface 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

Before you can configure the maximum number of connections, TCP header compression must be configured on the interface using the **frame-relay ip tcp header-compression** command.

The number of TCP header compression connections must be set to the same value at each end of the connection.

Examples

The following example shows the configuration of a maximum of 150 TCP header compression connections on serial interface 0:

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip tcp header-compression
 frame-relay ip tcp compression-connections 150
```

Related Commands

Command	Description
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
frame-relay map ip tcp header-compression	Assigns header compression characteristics to an IP map that differ from the compression characteristics of the interface with which the IP map is associated.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay ip tcp header-compression

To configure an interface to ensure that the associated permanent virtual circuit (PVC) will always carry outgoing TCP/IP headers in compressed form, use the **frame-relay ip tcp header-compression** command in interface configuration mode. To disable compression of TCP/IP packet headers on the interface, use the **no** form of this command.

frame-relay ip tcp header-compression [**passive**]

no frame-relay ip tcp header-compression

Syntax Description

passive	(Optional) Compresses the outgoing TCP/IP packet header only if an incoming packet had a compressed header.

Command Default

Active TCP/IP header compression; all outgoing TCP/IP packets are subjected to header compression.

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

This command applies to interfaces that support Frame Relay encapsulation, specifically serial ports and High-Speed Serial Interface (HSSI).

Frame Relay must be configured on the interface before this command can be used.

TCP/IP header compression and Internet Engineering Task Force (IETF) encapsulation are mutually exclusive. If an interface is changed to IETF encapsulation, all encapsulation and compression characteristics are lost.

When you use this command to enable TCP/IP header compression, every IP map inherits the compression characteristics of the interface, unless header compression is explicitly rejected or modified by use of the **frame-relay map ip tcp header compression** command.

We recommend that you shut down the interface prior to changing encapsulation types. Although this is not required, shutting down the interface ensures the interface is reset for the new type.

Examples

The following example configures serial interface 1 to use the default encapsulation (cisco) and passive TCP header compression:

```
interface serial 1
 encapsulation frame-relay
 frame-relay ip tcp header-compression passive
```

Related Commands

Command	Description
frame-relay map ip tcp header-compression	Assigns header compression characteristics to an IP map different from the compression characteristics of the interface with which the IP map is associated.

frame-relay lapf frmr

To resume the default setting of sending the Frame Reject (FRMR) frame at the Link Access Procedure for Frame Relay (LAPF) Frame Reject procedure after having set the option of not sending the frame, use the **frame-relay lapf frmr** command in interface configuration mode. To set the option of *not* sending the Frame Reject (FRMR) frame at the LAPF Frame Reject procedure, use the **no** form of this command.

frame-relay lapf frmr

no frame-relay lapf frmr

Syntax Description

This command has no arguments or keywords.

Defaults

Send FRMR during the Frame Reject procedure.

Command Modes

Interface configuration

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

If the Frame Relay switch does not support FRMR, use the **no** form of this command to suppress the transmission of FRMR frames.

Examples

The following example suppresses the transmission of FRMR frames:

```
no frame-relay lapf frmr
```

frame-relay lapf k

To set the Link Access Procedure for Frame Relay (LAPF) window size *k*, use the **frame-relay lapf k** command in interface configuration mode. To reset the maximum window size *k* to the default value, use the **no** form of this command.

frame-relay lapf k *number*

no frame-relay lapf k [*number*]

Syntax Description

number	Maximum number of Information frames that either are outstanding for transmission or are transmitted but unacknowledged, in the range from 1 to 127.

Defaults

7 frames

Command Modes

Interface configuration

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

This command is used to tune Layer 2 system parameters to work well with the Frame Relay switch. Normally, you do not need to change the default setting.

Manipulation of Layer 2 parameters is not recommended if you do not know well the resulting functional change. For more information, refer to the ITU-T Q.922 specification for LAPF.

Examples

The following example resets the LAPF window size *k* to the default value:

```
no frame-relay lapf k
```

Related Commands

Command	Description
frame-relay lapf t203	Sets the LAPF link idle timer value T203 of DLCI 0.

frame-relay lapf n200

To set the Link Access Procedure for Frame Relay (LAPF) maximum retransmission count N200, use the **frame-relay lapf n200** command in interface configuration mode. To reset the maximum retransmission count to the default of 3, use the **no** form of this command.

frame-relay lapf n200 *retries*

no frame-relay lapf n200 [*retries*]

Syntax Description

retries	Maximum number of retransmissions of a frame.

Defaults

3 retransmissions

Command Modes

Interface configuration

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

This command is used to tune Layer 2 system parameters to work well with the Frame Relay switch. Normally, you do not need to change the default setting.

Manipulation of Layer 2 parameters is not recommended if you do not know well the resulting functional change. For more information, refer to the ITU-T Q.922 specification for LAPF.

Examples

The following example resets the N200 maximum retransmission count to the default value:

```
no frame-relay lapf n200
```

frame-relay lapf n201

To set the Link Access Procedure for Frame Relay (LAPF) N201 value (the maximum length of the Information field of the LAPF I frame), use the **frame-relay lapf n201** command in interface configuration mode. To reset the maximum length of the Information field to the default of 260 bytes (octets), use the **no** form of this command.

frame-relay lapf n201 *bytes*

no frame-relay lapf n201 [*bytes*]

Syntax Description

bytes	Maximum number of bytes in the Information field of the LAPF I frame. Range is from 1 to 16384. Default is 260.

Defaults

260 bytes

Command Modes

Interface configuration

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

This command is used to tune Layer 2 system parameters to work well with the Frame Relay switch. Normally, you do not need to change the default setting.

Manipulation of Layer 2 parameters is not recommended if you do not know well the resulting functional change. For more information, refer to the ITU-T Q.922 specification for LAPF.

Examples

The following example resets the N201 maximum information field length to the default value:

```
no frame-relay lapf n201
```

frame-relay lapf t200

To set the Link Access Procedure for Frame Relay (LAPF) retransmission timer value T200, use the **frame-relay lapf t200** command in interface configuration mode. To reset the T200 timer to the default value of 15, use the **no** form of this command.

frame-relay lapf t200 *tenths-of-a-second*

no frame-relay lapf t200

Syntax Description

tenths-of-a-second	Time, in tenths of a second. Range is from 1 to 100. Default is 15.

Defaults

15 tenths of a second (1.5 seconds)

Command Modes

Interface configuration

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

The retransmission timer value T200 should be less than the link idle timer value T203 (using the same time unit).

This command is used to tune Layer 2 system parameters to work well with the Frame Relay switch. Normally, you do not need to change the default setting.

Manipulation of Layer 2 parameters is not recommended if you do not know well the resulting functional change. For more information, refer to the ITU-T Q.922 specification for LAPF.

Examples

The following example resets the T200 timer to the default value:

```
no frame-relay lapf t200
```

Related Commands

Command	Description
frame-relay lapf t203	Sets the LAPF link idle timer value T203 of DLCI 0.

frame-relay lapf t203

To set the Link Access Procedure for Frame Relay (LAPF) link idle timer value T203 of data-link connection identifier (DLCI) 0, use the **frame-relay lapf t203** command in interface configuration mode. To reset the link idle timer to the default value, use the **no** form of this command.

frame-relay lapf t203 *seconds*

no frame-relay lapf t203

Syntax Description

seconds	Maximum time allowed with no frames exchanged. Range is from 1 to 65535 seconds. Default is 30.

Defaults

30 seconds

Command Modes

Interface configuration

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

The **frame-relay lapf t203** command applies to the link; that is, it applies to DLCI 0. Circuits other than DLCI 0 are not affected.

The link idle timer value T203 should be greater than the retransmission timer value T200 (using the same time unit).

This command is used to tune Layer 2 system parameters to work well with the Frame Relay switch. Normally, you do not need to change the default setting.

Manipulation of Layer 2 parameters is not recommended if you do not know well the resulting functional change. For more information, refer to the ITU-T Q.922 specification for LAPF.

Examples

The following example resets the T203 idle link timer to the default value:

```
no frame-relay lapf t203
```

frame-relay lmi-n391dte

To set a full status polling interval, use the **frame-relay lmi-n391dte** command in interface configuration mode. To restore the default interval value, assuming that a Local Management Interface (LMI) has been configured, use the **no** form of this command.

frame-relay lmi-n391dte *keep-exchanges*

no frame-relay lmi-n391dte *keep-exchanges*

Syntax Description

keep-exchanges	Number of keep exchanges to be done before requesting a full status message. Acceptable value is a positive integer in the range from 1 to 255.

Defaults

6 keep exchanges

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

Use this command when the interface is configured as data terminal equipment (DTE) or a Network-to-Network Interface (NNI) as a means of setting the full status message polling interval.

Examples

In the following example, one out of every four status inquiries generated will request a full status response from the switch. The other three status inquiries will request keepalive exchanges only.

```
interface serial 0
 frame-relay intf-type DTE
 frame-relay lmi-n391dte 4
```

frame-relay lmi-n392dce

To set the DCE and the Network-to-Network Interface (NNI) error threshold, use the **frame-relay lmi-n392dce** command in interface configuration mode. To remove the current setting, use the **no** form of this command.

frame-relay lmi-n392dce *threshold*

no frame-relay lmi-n392dce *threshold*

Syntax Description

threshold	Error threshold value. Acceptable value is a positive integer in the range from 1 to 10.

Defaults

2 errors

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

In Cisco's implementation, N392 errors must occur within the number defined by the N393 event count in order for the link to be declared down. Therefore, the threshold value for this command must be less than the count value defined in the **frame-relay lmi-n393dce** command.

Examples

The following example sets the LMI failure threshold to 3. The router acts as a Frame Relay DCE or NNI switch.

```
interface serial 0
 frame-relay intf-type DCE
 frame-relay lmi-n392dce 3
```

Related Commands

Command	Description
frame-relay lmi-n393dce	Sets the DCE and NNI monitored events count.

frame-relay lmi-n392dte

To set the error threshold on a DTE or network-to-network interface (NNI) interface, use the **frame-relay lmi-n392dte** command in interface configuration mode. To remove the current setting, use the **no** form of this command.

frame-relay lmi-n392dte *threshold*

no frame-relay lmi-n392dte *threshold*

Syntax Description

threshold	Error threshold value. Acceptable value is a positive integer in the range from 1 to 10.

Defaults

3 errors

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.

Examples

The following example sets the Local Management Interface (LMI) failure threshold to 3. The router acts as a Frame Relay DTE or NNI switch.

```
interface serial 0
 frame-relay intf-type DTE
 frame-relay lmi-n392dte 3
```

frame-relay lmi-n393dce

To set the DCE and Network-to-Network Interface (NNI) monitored events count, use the **frame-relay lmi-n393dce** command in interface configuration mode. To remove the current setting, use the **no** form of this command.

frame-relay lmi-n393dce *events*

no frame-relay lmi-n393dce *events*

Syntax Description

events	Value of monitored events count. Acceptable value is a positive integer in the range from 1 to 10.

Defaults

2 events

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

This command and the **frame-relay lmi-n392dce** command define the condition that causes the link to be declared down. In Cisco's implementation, N392 errors must occur within the *events* argument count in order for the link to be declared down. Therefore, the *events* value defined in this command must be greater than the threshold value defined in the **frame-relay lmi-n392dce** command.

Examples

The following example sets the Local Management Interface (LMI) monitored events count to 3. The router acts as a Frame Relay DCE or NNI switch.

```
interface serial 0
 frame-relay intf-type DCE
 frame-relay lmi-n393dce 3
```

Related Commands

Command	Description
frame-relay lmi-n392dce	Sets the DCE and the NNI error threshold.

frame-relay lmi-n393dte

To set the monitored event count on a DTE or Network-to-Network Interface (NNI) interface, use the **frame-relay lmi-n393dte** command in interface configuration mode. To remove the current setting, use the **no** form of this command.

frame-relay lmi-n393dte *events*

no frame-relay lmi-n393dte *events*

Syntax Description

events	Value of monitored events count. Acceptable value is a positive integer in the range from 1 to 10.

Defaults

4 events

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.

Examples

The following example sets the Local Management Interface (LMI) monitored events count to 3. The router acts as a Frame Relay DTE or NNI switch.

```
interface serial 0
 frame-relay intf-type DTE
 frame-relay lmi-n393dte 3
```

frame-relay lmi-t392dce

To set the polling verification timer on a DCE or Network-to-Network Interface (NNI) interface, use the **frame-relay lmi-t392dce** command in interface configuration mode. To remove the current setting, use the **no** form of this command.

frame-relay lmi-t392dce *seconds*

no frame-relay lmi-t392dce *seconds*

Syntax Description

seconds	Polling verification timer value from 5 to 30 seconds.

Defaults

15 seconds

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

The value for the timer must be greater than the DTE or NNI keepalive timer.

Examples

The following example indicates a polling verification timer on a DCE or NNI interface set to 20 seconds:

```
interface serial 3
 frame-relay intf-type DCE
 frame-relay lmi-t392dce 20
```

Related Commands

Command	Description
keepalive (LMI)	Enables the LMI mechanism for serial lines using Frame Relay encapsulation.

frame-relay lmi-type

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** command in interface configuration mode. To return to the default LMI type, use the **no** form of this command.

frame-relay lmi-type {**ansi** | **cisco** | **q933a**}

no frame-relay lmi-type {**ansi** | **q933a**}

Syntax Description

ansi	Annex D defined by American National Standards Institute (ANSI) standard T1.617.
cisco	LMI type defined jointly by Cisco and three other companies.
q933a	ITU-T Q.933 Annex A.

Defaults

LMI autosense is active and determines the LMI type by communicating with the switch.

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

Cisco's implementation of Frame Relay supports three LMI types: Cisco, ANSI Annex D, and ITU-T Q.933 Annex A.

The LMI type is set on a per-interface basis and is shown in the output of the **show interfaces** EXEC command.

If you want to deactivate LMI autosense, use this command and the **keepalive** command to configure the LMI. For more information about LMI autosense and configuring the LMI, refer to the chapter "Configuring Frame Relay" in the *Cisco IOS Wide-Area Networking Configuration Guide*.

Examples

The following is an example of the commands you might enter to configure an interface for the ANSI Annex D LMI type:

```
interface Serial1
 encapsulation frame-relay
 frame-relay lmi-type ansi
 keepalive 15
```

frame-relay local-dlci

To set the source data-link connection identifier (DLCI) for use when the Local Management Interface (LMI) is not supported, use the **frame-relay local-dlci** command in interface configuration mode. To remove the DLCI number, use the **no** form of this command.

frame-relay local-dlci *number*

no frame-relay local-dlci

Syntax Description

number	Local (source) DLCI number to be used.

Defaults

No source DLCI is set.

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

If LMI is supported and the multicast information element is present, the network server sets its local DLCI based on information provided via the LMI.

Note The **frame-relay local-dlci** command is provided mainly to allow testing of the Frame Relay encapsulation in a setting where two servers are connected back-to-back. This command is not required in a live Frame Relay network.

Examples

The following example specifies 100 as the local DLCI:

```
interface serial 4
 frame-relay local-dlci 100
```

frame-relay map

To define the mapping between a destination protocol address and the data-link connection identifier (DLCI) or Frame Relay permanent virtual circuit (PVC) bundle that connects to the destination address, use the **frame-relay map** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map *protocol protocol-address* {*dlci* | **vc-bundle** *vc-bundle-name*}[**broadcast**] [**ietf** | **cisco**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [**one-way-negotiation**] [**ratio** *level*] [**skip-zero-sync**] [**software** | *hardware-options*] | **data-stream stac** [**one-way-negotiation**] [**ratio** *level*] [**software** | *hardware-options*]}]

no frame-relay map *protocol protocol-address*

Syntax Description

protocol	One of the following values: **appletalk**, **decnet**, **dlsw, ip**, **ipx**, **llc2**, and **rsrb**.
protocol-address	Destination protocol address.
dlci	DLCI number used to connect to the specified protocol address on the interface. Acceptable numbers are integers from 16 through 1007, inclusive.
vc-bundle *vc-bundle-name*	A specific Frame Relay PVC bundle configured on the interface.
broadcast	(Optional) Forwards broadcasts to this address when multicast is not enabled (see the **frame-relay multicast-dlci** command for more information about multicasts). This keyword also simplifies the configuration of Open Shortest Path First (OSPF) (see the "Usage Guidelines" section for more detail).
ietf	(Optional) Internet Engineering Task Force (IETF) form of Frame Relay encapsulation, based on RFC 1490 and RFC 2427. Used when the router or access server is connected to another vendor's equipment across a Frame Relay network.
cisco	(Optional) Cisco-proprietary encapsulation method consisting of a four-byte header, with two bytes to identify the DLCI and two bytes to identify the packet type.
payload-compression	(Optional) Enables payload compression.
packet-by-packet	(Optional) Packet-by-packet payload compression using the Stacker method.
frf9 stac	(Optional) Enables FRF.9 compression using the Stacker method. • If the router contains a CSA[1], compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the VIP2[2] (distributed compression). • If the VIP2 is not available, compression is performed in the main processor of the router (software compression).

one-way-negotiation	(Optional) Enables one-way negotiation. Use this keyword if your router will be negotiating compression with another device that is running Cisco IOS Release 12.1(9) or earlier releases. Later Cisco IOS releases use a two-way handshake by default to negotiate compression.
ratio *level*	(Optional) Sets throughput versus compression ratio. This option is available only with hardware compression. Possible values for the *level* argument are as follows: **high**—high compression versus low throughput **medium**—medium compression versus medium throughput **low**—low compression versus high throughput (default)
software	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router.
hardware-options	(Optional) Choose one of the following hardware options: **caim** *element-number*—Enables the CAIM[3] to perform compression. **distributed**—Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. **csa** *csa_number*—Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.
skip-zero-sync	(Optional) Causes compression frames to be numbered starting from 1 rather than 0. Use this keyword if your router will be interoperating with a device conforming to IBM partner conventions.
data-stream stac	(Optional) Enables data-stream compression using the Stacker method. • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression).

1. CSA = compression service adapter
2. VIP2 = second-generation Versatile Interface Processor
3. CAIM = compression Advanced Interface Module

Defaults

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **payload-compress frf9 stac** keyword was added.
12.1(5)T	The **payload-compress data-stream stac** keyword was added.
12.2(4)T	The **skip-zero-sync** keyword was added.
12.2(13)T	The **vc-bundle** *vc-bundle-name* keyword and argument pair was added. The **apollo**, **vines**, and **xns** arguments were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer available in the Cisco IOS software. The **one-way-negotiation** keyword was added.
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.

Usage Guidelines

Many DLCIs can be known by a router or access server and can send data to many different places, but they are all multiplexed over one physical link. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI or PVC bundle.

The optional **ietf** and **cisco** keywords allow flexibility in the configuration. If no keywords are specified, the map inherits the attributes set with the **encapsulation frame-relay** command. You can also use the encapsulation options to specify, for example, that all interfaces use IETF encapsulation except one, which needs the original Cisco encapsulation method and can be configured through use of the **cisco** keyword with the **frame-relay map** command.

Data-stream compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keyword is specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on IETF-encapsulated VCs and interfaces. When the **frf9 stac** keyword is specified, IETF encapsulation is automatically enabled.

Packet-by-packet compression is Cisco-proprietary and will not interoperate with routers of other manufacturers.

You can disable payload compression by entering the **no frame-relay map payload** command and then entering the **frame-relay map** command again with one of the other encapsulation keywords (**ietf** or **cisco**).

Use the **frame-relay map** command to enable or disable payload compression on multipoint interfaces. Use the **frame-relay payload-compression** command to enable or disable payload compression on point-to-point interfaces.

We recommend that you shut down the interface before changing encapsulation types. Although shutting down the interface is not required, it ensures that the interface is reset for the new encapsulation.

The **broadcast** keyword provides two functions: it forwards broadcasts when multicasting is not enabled, and it simplifies the configuration of OSPF for nonbroadcast networks that will use Frame Relay.

The **broadcast** keyword may also be required for some routing protocols—for example, AppleTalk—that depend on regular routing table updates, especially when the router at the remote end is waiting for a routing update packet to arrive before adding the route.

By requiring selection of a designated router, OSPF treats a nonbroadcast, multiaccess network such as Frame Relay in much the same way as it treats a broadcast network. When the **frame-relay map** command (with the **broadcast** keyword) and the **ip ospf network** command (with the **broadcast** keyword) are configured, there is no need to configure any neighbors manually. OSPF will run automatically over the Frame Relay network as a broadcast network. (See the **ip ospf network** interface command for more detail.)

Note The OSPF broadcast mechanism assumes that IP class D addresses are never used for regular traffic over Frame Relay.

Examples

IP Address to DLCI Mapping: Example

The following example maps the destination IP address 172.16.123.1 to DLCI 100:

```
interface serial 0
 frame-relay map ip 172.16.123.1 100 broadcast
```

OSPF will use DLCI 100 to broadcast updates.

IP Address to Frame Relay PVC Bundle Mapping: Example

The following example maps the destination IP address 172.16.123.1 to the Frame Relay PVC bundle named “MAIN-1”:

```
interface serial 0
 frame-relay map ip 172.16.123.1 vc-bundle MAIN-1 broadcast
```

FRF.9 Compression: Example

The following example shows FRF.9 compression configuration using the **frame-relay map** command:

```
interface serial2/0/1
 ip address 172.16.1.4 255.255.255.0
 no ip route-cache
 encapsulation frame-relay ietf
 no keepalive
 shutdown
 frame-relay map ip 172.16.1.1 105 ietf payload-compression frf9 stac
```

Data-Stream Compression: Example

The following example shows data-stream compression configuration using the **frame-relay map** command:

```
interface serial0/0
 frame-relay map ip 10.0.0.1 100 payload-compression data-stream stac
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation on an interface.
frame-relay payload-compression	Enables Stacker payload compression on a specified point-to-point interface or subinterface.
frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.

frame-relay map bridge

To specify that broadcasts are to be forwarded during bridging, use the **frame-relay map bridge** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map bridge *dlci* [**broadcast**] [**ietf**]

no frame-relay map bridge *dlci*

Syntax Description

dlci	DLCI number to be used for bridging on the specified interface or subinterface.
broadcast	(Optional) Broadcasts are forwarded when multicast is not enabled.
ietf	(Optional) IETF form of Frame Relay encapsulation. Use when the router or access server is connected to another vendor's equipment across a Frame Relay network.

Defaults

No broadcasts are forwarded.

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.
12.4(13)	This command was modified to remove support for bridging for Frame Relay permanent virtual circuit (PVC) bundles.
12.0(32)SY3	This command was modified to remove support for bridging for Frame Relay PVC bundles.
12.4(15)T	This command was modified to remove support for bridging for Frame Relay PVC bundles.
12.2(14)S11b	This command was modified to remove support for bridging for Frame Relay PVC bundles.
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.
12.0(33)S	This command was modified to remove support for bridging for Frame Relay PVC bundles.
12.2(33)SRC	This command was modified to remove support for bridging for Frame Relay PVC bundles.
12.2(44)SQ	This command was modified to remove support for bridging for Frame Relay PVC bundles.

Examples

The following example uses DLCI 144 for bridging:

```
interface serial 0
 frame-relay map bridge 144 broadcast
```

The following example sets up separate point-to-point links over a subinterface and runs transparent bridging over it:

```
interface serial 0
 bridge-group 1
 encapsulation frame-relay
interface serial 0.1
 bridge-group 1
 frame-relay map bridge 42 broadcast
interface serial 0.2
 bridge-group 1
 frame-relay map bridge 64 broadcast
interface serial 0.3
 bridge-group 1
 frame-relay map bridge 73 broadcast
```

DLCI 42 is used as the link; refer to the section “Frame Relay Configuration Examples” in the *Cisco IOS Wide-Area Networking Configuration Guide* for more examples of subinterfaces.

frame-relay map clns

To forward broadcasts when Connectionless Network Service (CLNS) is used for routing, use the **frame-relay map clns** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map clns *dlci* [**broadcast**]

no frame-relay map clns *dlci*

Syntax Description

dlci	DLCI number to which CLNS broadcasts are forwarded on the specified interface.
broadcast	(Optional) Broadcasts are forwarded when multicast is not enabled.

Defaults

No broadcasts are forwarded.

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.

Examples

The following example uses DLCI 125 for CLNS routing:

```
interface serial 0
 frame-relay map clns 125 broadcast
```

frame-relay map ip tcp header-compression

To assign to an IP map header compression characteristics that differ from the compression characteristics of the interface with which the IP map is associated, use the **frame-relay map ip tcp header-compression** command in interface configuration mode.

frame-relay map ip *ip-address dlci* [**broadcast**] **tcp header-compression** [**active** | **passive**] [**connections** *number*]

Syntax Description

ip-address	IP address of the destination or next hop.
dlci	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.
active	(Optional) Compresses the header of every outgoing TCP/IP packet.
passive	(Optional) Compresses the header of an outgoing TCP/IP packet only if an incoming TCP/IP packet had a compressed header.
connections *number*	(Optional) Specifies the maximum number of TCP header compression connections. The range is from 3 to 256. Default is 256.

Defaults

Maximum number of TCP header compression connections: 256

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.
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

If you do not specify the number of TCP header compression connections, the map will inherit the current value from the interface.

IP maps inherit the compression characteristics of the associated interface unless this command is used to provide different characteristics. This command can also reconfigure an IP map that existed before TCP header compression was configured on the associated interface.

When IP maps at both ends of a connection inherit passive compression, the connection will never transfer compressed traffic because neither side will generate a packet that has a compressed header.

If you change the encapsulation characteristics of the interface to Internet Engineering Task Force (IETF) encapsulation, you lose the TCP header compression configuration of the associated IP map.

The **frame-relay map ip** *ip-address dlci* **tcp header-compression active** command can also be entered as **frame-relay map ip** *ip-address dlci* **active tcp header-compression**.

We recommend that you shut down the interface before changing encapsulation types. Although shutting down the interface is not required, it ensures that the interface is reset for the new encapsulation.

Examples

The following example illustrates a command sequence for configuring an IP map associated with serial interface 1 to enable active TCP/IP header compression:

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.177.170 255.255.255.0
 frame-relay map ip 10.108.177.180 190 tcp header-compression active
```

Related Commands

Command	Description
frame-relay ip tcp compression-connections	Specifies the maximum number of TCP header compression connections that can exist on a Frame Relay interface.
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay mincir

To specify the minimum acceptable incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit, use the **frame-relay mincir** command in map-class configuration mode. To reset the minimum acceptable CIR to the default, use the **no** form of this command.

frame-relay mincir {**in** | **out**} *bps*

no frame-relay mincir

Syntax Description

in	Specifies an incoming CIR.
out	Specifies an outgoing CIR.
bps	Rate, in bits per second.

Defaults

56000 bps

Command Modes

Map-class configuration

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.
Cisco IOS XE Release 2.6	This command was modified. This command is no longer valid for permanent virtual circuits (PVCs).
15.0(1)S	This command was modified. This command is no longer valid for PVCs.
15.1(3)T	This command was modified. This command is no longer valid for PVCs.

Usage Guidelines

Rate values greater than 2048 must be entered with trailing zeros. For example, 2048000 and 5120000.

The network uses the **mincir** value when allocating resources for the virtual circuit. If the **mincir** value cannot be supported, the call is cleared.

Examples

The following example defines the peak and average traffic rate, the minimum CIR, and the idle timer for the fast_vcs map class and applies those values to DLCI 100, which is associated with that map class:

```
interface serial 0
 frame-relay interface-dlci 100
  class fast_vc

map-class frame-relay fast_vc
 frame-relay traffic-rate 56000 128000
 frame-relay idle-timer 30
 frame-relay mincir out 48000
```

Related Commands

Command	Description
map-class frame-relay	Specifies a map class to define QoS values for virtual circuits.

frame-relay multicast-dlci

To define the data-link connection identifier (DLCI) to be used for multicasts, use the **frame-relay multicast-dlci** command in interface configuration mode. To remove the multicast group, use the **no** form of this command.

frame-relay multicast-dlci *number*

no frame-relay multicast-dlci

Syntax Description

number	Multicast DLCI.

Defaults

No DLCI is defined.

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

Use this command when the multicast facility is not supported. Network transmissions (packets) sent to a multicast DLCI are delivered to all network servers defined as members of the multicast group.

Note The **frame-relay multicast-dlci** command is provided mainly to allow testing of the Frame Relay encapsulation in a setting where two servers are connected back-to-back. This command is not required in a live Frame Relay network.

Examples

The following example specifies 1022 as the multicast DLCI:

```
interface serial 0
 frame-relay multicast-dlci 1022
```

frame-relay multilink ack

To configure the number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message, use the **frame-relay multilink ack** command in interface configuration mode. To reset this parameter to the default setting, use the **no** form of this command.

frame-relay multilink ack *seconds*

no frame-relay multilink ack

Syntax Description

seconds	Number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message. Range: 1 to 10. Default: 4.

Command Default

The default acknowledgement interval is 4 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 **frame-relay multilink ack** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The **frame-relay multilink ack** command setting on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure the bundle link to wait 6 seconds before resending hello messages:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink ack 6
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink hello	Configures the interval at which a bundle link will send out hello messages.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink bandwidth-class

To specify the criterion used to activate or deactivate a Frame Relay bundle, use the **frame-relay multilink bandwidth-class** command in interface configuration mode. To reset the bandwidth class to the default, use the **no** form of this command.

frame-relay multilink bandwidth-class [**a** | **b** | **c** [*threshold*]]

no frame-relay multilink bandwidth-class

Syntax Description

a	(Optional) Bandwidth class A (single link) criterion will be used to activate or deactivate the Frame Relay bundle. This is the default. • Criterion for activation—One or more bundle links indicate (by issuing a BL_ACTIVATE message) that operational bandwidth is available. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation—All bundle links are down and issue a BL_DEACTIVATE message, which triggers a PH_DEACTIVATE message to be sent to the data-link layer, indicating that the Frame Relay bundle cannot accept frames.
b	(Optional) Bandwidth class B (all links) criterion will be used to activate or deactivate the Frame Relay bundle. • Criterion for activation—All bundle links indicate (by issuing a BL_ACTIVATE message) that operational bandwidth is available. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation—Any bundle link is down and issues a BL_DEACTIVATE message, which triggers a PH_DEACTIVATE message to be sent to the data-link layer, indicating that the Frame Relay bundle cannot accept frames.
c	(Optional) Bandwidth class C (threshold) criterion will be used to activate or deactivate the Frame Relay bundle. • Criterion for activation—The minimum number of links in the configured bundle issue a BL_ACTIVATE message. When this occurs, the bundle emulates a physical link by issuing a PH_ACTIVATE message to the data-link layer. • Criterion for deactivation—The number of bundle links issuing a BL_ACTIVATE message falls below the configured *threshold* value. When this occurs, a PH_DEACTIVATE message is sent to the data-link layer, which indicates that the Frame Relay bundle cannot accept frames.
threshold	(Optional) Number of bundle links. The range is from 1 to 65535. If the *threshold* argument is not specified, the default value is 1.

Command Default

Frame Relay bundles use bandwidth class A (single link).

Command Modes Interface configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.

Usage Guidelines The **frame-relay multilink bandwidth-class** command can be configured only on a bundle's main interface. If no bandwidth class is specified by using the **frame-relay multilink bandwidth-class** command, the Frame Relay bundle uses the class A (single link) criterion.

Examples The following example shows how to specify the class B (all links) bandwidth class to trigger activation or deactivation of the Frame Relay bundle on MFR interface 0:

```
interface mfr0
 frame-relay multilink bandwidth-class b
```

The following example shows how to specify the class C (threshold) bandwidth class to trigger activation or deactivation of the Frame Relay bundle on MFR interface 0, where the minimum threshold of links indicating BL_ACTIVATE is 3:

```
interface mfr0
 frame-relay multilink bandwidth-class c 3
```

Related Commands

Command	Description
interface mfr	Configures a multilink Frame Relay bundle interface.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

frame-relay multilink bid

To assign a bundle identification (BID) name to a multilink Frame Relay bundle, use the **frame-relay multilink bid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink bid *name*

no frame-relay multilink bid

Syntax Description

name	Bundle identification (BID) name. The name can be up to 49 characters long. The default is "mfr" followed by the number assigned to the bundle using the **interface mfr** command; for example, "mfr0."

Command Default

The BID name is assigned automatically as "mfr" followed by the number assigned to the bundle.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 can be entered only on the multilink Frame Relay bundle interface.

Note You can enter the **frame-relay multilink bid** command at any time without affecting the current state of the interface; however, the BID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Only one BID is allowed per bundle. A later entry of the **frame-relay multilink bid** command supersedes prior entries.

The local and peer BIDs do not have to be unique.

Examples

The following example shows how to assign a BID of “bundle1” to the multilink Frame Relay bundle. The previous BID for the bundle was “mfr0.”

```
interface mfr0
 frame-relay multilink bid bundle1
```

Related Commands

Command	Description
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
interface mfr	Configures a multilink Frame Relay bundle interface.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay multilink hello

To configure the interval at which a bundle link will send out hello messages, use the **frame-relay multilink hello** command in interface configuration mode. To reset this value to the default setting, use the **no** form of this command.

frame-relay multilink hello *seconds*

no frame-relay multilink hello

Syntax Description

seconds	Interval, in seconds, at which a bundle link will send out hello messages. Range: 1 to 180. Default: 10.

Command Default

The interval is set at 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 **frame-relay multilink hello** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The setting of the hello message interval on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure a bundle link to send hello messages every 15 seconds:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink hello 15
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink ack	Configures the number of seconds that a bundle link will wait for a hello message acknowledgment before resending the hello message.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink lid

To assign a bundle link identification (LID) name to a multilink Frame Relay bundle link, use the **frame-relay multilink lid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink lid *name*

no frame-relay multilink lid

Syntax Description

name	Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

The name of the physical interface is used as the LID.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 **frame-relay multilink lid** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink lid** command at any time without affecting the current state of the interface; however, the LID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

The LID will be used to identify the bundle link to peer devices and to enable the devices to identify which bundle links are associated with which bundles. The LID can also be assigned when the bundle link is created by using the **encapsulation frame-relay mfr** command with the *name* argument. If the LID is not assigned, the default LID is the name of the physical interface. The local and peer LIDs do not have to be unique.

Examples

The following example shows the LID named BL1 assigned to serial interface 0:

```
interface serial 0
 encapsulation frame-relay mfr0
 frame-relay multilink lid BL1
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay multilink output-threshold

To configure the number of bytes that a bundle link will transmit before the load-balancing mechanism causes transmission to roll over to the next available link, use the **frame-relay multilink output-threshold** command in interface configuration mode. To reset this value to the default setting, use the **no** form of this command.

frame-relay multilink output-threshold *bytes*

no frame-relay multilink output-threshold

Syntax Description

bytes	Number of bytes that a bundle link will transmit before the load-balancing mechanism causes transmission to roll over to the next link. Range: 20 to 2147483647. Default: 300.

Command Default

The number of bytes transmitted is set at 300.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)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.
12.2(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

Multilink Frame Relay enables load balancing across bundle links that are in the same bundle. When a bundle link has reached its output threshold, transmission rolls over to the next available bundle link in the bundle.

The output threshold mechanism applies only when the bundle interface is using FIFO output queueing. When the bundle interface is not using FIFO output queuing, the algorithm for choosing a bundle link interface for output selects the bundle link that has the empty or shortest output queue.

The default output threshold is 300 bytes. This default value will work effectively if all the bundle links in the bundle have the same speed. To efficiently use bundle links with different speeds, use the **frame-relay multilink output-threshold** command to adjust the output threshold of the links as appropriate.

The **frame-relay multilink output-threshold** command can be used on the bundle interface and the bundle links. If the command is used on the bundle interface, the configured output threshold will apply to all bundle links in the bundle. If the command is used on a specific bundle link, the output threshold will overwrite the current setting for that bundle link.

Examples

The following example shows how to configure the bundle link output threshold at 600 bytes. When the bundle link reaches the threshold, transmission will roll over to the next link.

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink output-threshold 600
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.

frame-relay multilink retry

To configure the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment, use the **frame-relay multilink retry** command in interface configuration mode. To reset this value to the default setting, use the **no** form of this command.

frame-relay multilink retry *number*

no frame-relay multilink retry

Syntax Description

number	Maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment. Range: 1 through 5. Default: 2.

Command Default

The number of retries is set at 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
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.

Usage Guidelines

The **frame-relay multilink retry** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

If the bundle link sends the maximum number of hello messages without receiving an acknowledgment, the bundle link line protocol is considered down (nonoperational).

The maximum number of retries configured on the local router is independent of the maximum number configured on the peer device.

Examples

The following example shows how to configure a bundle link to send a hello message a maximum of 3 times while waiting for an acknowledgment:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink retry 3
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink ack	Configures the number of seconds that a bundle link will wait for a hello message acknowledgment before resending the hello message.
frame-relay multilink hello	Configures the interval at which a bundle link will send out hello messages.

frame-relay payload-compression

To enable Stacker payload compression on a specified point-to-point interface or subinterface, use the **frame-relay payload-compression** command in interface configuration mode. To disable payload compression on a specified point-to-point interface or subinterface, use the **no** form of this command.

frame-relay payload-compression {**packet-by-packet** | **frf9 stac** [**one-way-negotiation**] [**ratio** *level*] [**skip-zero-sync**] [**software** | *hardware-options*] | **data-stream stac** [**one-way-negotiation**] [**ratio** *level*] [**software** | *hardware-options*]}

no frame-relay payload-compression {**packet-by-packet** | **frf9 stac | data-stream stac**}

Syntax Description

packet-by-packet	Packet-by-packet payload compression using the Stacker method.
frf9 stac	Enables FRF.9 compression using the Stacker method. • If the router contains a CSA[1], compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the VIP2[2] (distributed compression). • If the VIP2 is not available, compression is performed in the main processor of the router (software compression).
one-way-negotiation	(Optional) Enables one-way negotiation. Use this keyword if your router will be negotiating compression with another device that is running Cisco IOS Release 12.1(9) or earlier releases. Later Cisco IOS releases use a two-way handshake by default to negotiate compression.
ratio *level*	(Optional) Sets throughput versus compression ratio. This option is available only with hardware compression. Possible values for the *level* argument are as follows: **high**—high compression versus low throughput **medium**—medium compression versus medium throughput **low**—low compression versus high throughput (default)
skip-zero-sync	(Optional) Causes compression frames to be numbered starting from 1 rather than 0. Use this keyword if your router will be interoperating with a device that conforms to IBM partner conventions.
software	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router.

hardware-options	(Optional) Choose one of the following hardware options: **caim** *element-number*—Enables the CAIM[3] to perform compression. **distributed**—Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. **csa** *csa_number*—Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.
data-stream stac	Enables data-stream compression using the Stacker method. • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression).

1. CSA = compression service adapter
2. VIP2 = second-generation Versatile Interface Processor
3. CAIM = Compression Advanced Interface Module

Defaults

Payload compression is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The **packet-by-packet** keyword was added.
11.3	The **frf9 stac** keyword was added.
12.1(5)T	The **data-stream stac** keyword was added.
12.2(4)T	The **skip-zero-sync** keyword was added.
12.2(13)T	The **one-way-negotiation** keyword was 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

Use the **frame-relay payload-compression** command to enable or disable payload compression on a point-to-point interface or subinterface. Use the **frame-relay map** command to enable or disable payload compression on a multipoint interface or subinterface.

We recommend that you shut down the interface before changing encapsulation types. Although shutting down the interface is not required, it ensures that the interface is reset for the new encapsulation.

Data-stream hardware compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keyword is specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on VCs and interfaces that using Internet Engineering Task Force (IETF) encapsulation type. When the **frf9 stac** keyword is specified, IETF encapsulation is automatically enabled.

Examples

FRF.9 Compression: Example

The following example configures FRF.9 compression for subinterfaces:

```
interface serial2/0/0
 no ip address
 no ip route-cache
 encapsulation frame-relay
 ip route-cache distributed
 no keepalive
 shutdown
!
interface serial2/0/0.500 point-to-point
 ip address 172.16.1.4 255.255.255.0
 no cdp enable
 frame-relay interface-dlci 500 ietf
 frame-relay payload-compression frf9 stac
```

Data-Stream Compression: Example

The following example shows the configuration of data-stream compression using the **frame-relay payload-compression** command:

```
interface serial1/0
 encapsulation frame-relay
 frame-relay traffic-shaping
!
interface serial1/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 frame-relay interface-dlci 100
 frame-relay payload-compression data-stream stac
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.

frame-relay policing

To enable Frame Relay policing on all switched PVCs on the interface, use the **frame-relay policing** command in interface configuration mode. To disable Frame Relay policing, use the **no** form of this command.

frame-relay policing

no frame-relay policing

Syntax Description

This command has no arguments or keywords.

Defaults

Frame Relay policing is not enabled on switched PVCs.

Command Modes

Interface 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

You must enable Frame Relay policing on the incoming interface before you can configure traffic-policing parameters.

You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **frame-relay policing** command will be effective on switched PVCs.

Examples

The following example shows the configuration of Frame Relay policing on serial interface 0:

```
interface serial0
 frame-relay policing
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay virtual circuit.
frame-relay be	Specifies the incoming or outgoing Be for a Frame Relay virtual circuit.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay virtual circuit.
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
frame-relay tc	Specifies the measurement interval for policing incoming traffic when the CIR is zero.

frame-relay priority-dlci-group

To prioritize multiple data-link connection identifiers (DLCIs) according to the type of Frame Relay traffic, use the **frame-relay priority-dlci-group** interface configuration command.

frame-relay priority-dlci-group *group-number high-dlci medium-dlci normal-dlci low-dlci*

Syntax Description

group-number	Specific group number.
high-dlci	DLCI that is to have highest priority level.
medium-dlci	DLCI that is to have medium priority level.
normal-dlci	DLCI that is to have normal priority level.
low-dlci	DLCI that is to have lowest priority level.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	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

This command is applied at the interface or subinterface level. Levels in descending order are high, medium, normal, and low.

This command allows you to define different DLCIs for different categories of traffic based on traffic priorities. This command does not itself define priority queueing, but it can be used in conjunction with priority queueing.

A global priority list must be defined, and the associated DLCIs must already be applied to the configuration before you enable this command.

Associate the DLCIs to their prospective groups and define their priority levels. This command is used for multiple DLCIs, where the source and destination endpoints are the same (parallel paths). This command should not be used on a main interface, or point-to-point subinterface, where only a single DLCI is configured.

A DLCI can only be affiliated with a single priority-group; however, there can be multiple groups per interface or subinterface.

You must configure the *high-priority* and *medium-priority* DLCI values. If you do not explicitly associate a DLCI for the *normal-dlci* and *low-dlci* priority levels, the last DLCI specified in the command line is used as the value of the remaining arguments. For example, the following two commands are equivalent:

```
frame-relay priority-dlci-group 1 40 50
frame-relay priority-dlci-group 1 40 50 50 50
```

When you configure static map entries using **frame-relay map** commands or use Inverse Address Resolution Protocol (ARP), the high-level DLCI is the only DLCI that is mapped. In the example, DLCI 40 is defined as having the highest priority. Therefore, DLCI 40 is the only DLCI that should be included in the **frame-relay map** command. DLCI 50 should not be included in a **frame-relay map** command.

Examples

The following example shows the **frame-relay priority-dlci-group** command configured on a main interface with a static Frame Relay map entry. Note that DLCI 40 is the high-priority DLCI as defined in the **frame-relay priority-dlci-group** command and the only DLCI included in the **frame-relay map** command.

```
interface serial 1
 ip address 172.21.177.1 255.255.255.0
 encapsulation frame-relay
 frame-relay priority-dlci-group 1 40
 frame-relay map ip 172.21.177.2 40 broadcast
```

The following example shows the **frame-relay priority-dlci-group** command configured on subinterfaces where multiple priority groups are defined. DLCI 40 is the high-priority DLCI in group 1, and DLCI 80 is the high-priority DLCI in group 2.

```
interface Serial3
 no ip address
 encapsulation frame-relay
!
interface Serial3.2 multipoint
 ip address 172.21.177.1 255.255.255.0
 frame-relay interface-dlci 40
 frame-relay priority-dlci-group 1 40

!
interface Serial3.3 multipoint
 ip address 131.108.177.180 255.255.255.0
 frame-relay priority-dlci-group 2 80 90 100 100
 frame-relay interface-dlci 80
!
interface Serial 4
 no ip address
 encapsulation frame-relay
!
interface serial4.1 multipoint
 ip address 172.16.1.1 255.255.255.0
 frame-relay priority-dlci-group 3 200 210 300 300
 frame-relay priority-dlci-group 4 400 410 410 410
 frame-relay interface-dlci 200
 frame-relay interface-dlci 400
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.

frame-relay priority-group

Note Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relay priority-group** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay priority-group** command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To assign a priority queue to virtual circuits associated with a map class, use the **frame-relay priority-group** command in map-class configuration mode. To remove the specified queueing from the virtual circuit and cause it to revert to the default first-come, first-served queueing, use the **no** form of this command.

frame-relay priority-group *list-number*

no frame-relay priority-group *list-number*

Syntax Description

list-number	Priority-list number to be associated with the specified map class.

Defaults

If this command is not entered, the default is first-come, first-served queueing.

Command Modes

Map-class configuration

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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.

Release	Modification
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was replaced by an MQC command (or sequence of MQC commands).

Usage Guidelines

Use the **priority-list** commands to define the priority queue. Because only one form of queueing can be associated with a particular map class, subsequent definitions overwrite previous ones.

Examples

The following example configures a map class for a specified DLCI, specifies a priority list for the map class, and then defines the priority list:

```
interface serial 0
 encapsulation frame-relay
 frame-relay interface-dlci 100
 class pri_vc

 map-class frame-relay pri_vc
 frame-relay priority-group 1

priority-list 1 protocol ip high
```

Related Commands

Command	Description
class (virtual circuit)	Associates a map class with a specified DLCI.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay pvc

To configure Frame Relay permanent virtual circuits (PVCs) for FRF.8 Frame Relay-ATM Service Interworking, use the **frame-relay pvc** command in interface configuration mode. To remove the PVC, use the **no** form of the command.

frame-relay pvc *dlci* **service** {**transparent** | **translation**} [**clp-bit** {**0** | **1** | **map-de**}] [**de-bit** {**0** | **1** | **map-clp**}] [**efci-bit** {**0** | **1** | **map-fecn**}] **interface atm0** {*vpi*/*vci* | *vcd*}

no frame-relay pvc *dlci* **service** {**transparent** | **translation**} [**clp-bit** {**0** | **1** | **map-de**}] [**de-bit** {**0** | **1** | **map-clp**}] [**efci-bit** {**0** | **1** | **map-fecn**}] **interface atm0** {*vpi*/*vci* | *vcd*}

Syntax Description

dlci	A value ranging from 16 to 1007 for the PVC's data-link connection identifier (DLCI). Use this label when you associate a Frame Relay PVC with an ATM PVC.
service {**transparent** | **translation**}	In the **transparent** mode of Service Interworking, encapsulations are sent unaltered. In **translatio**n mode, mapping and translation take place. There is no default.
clp-bit {**0** | **1** | **map-de**}	(Optional) Sets the mode of DE/CLP mapping in Frame Relay to the ATM direction. The default is **map-de**. • **map-de**—Specifies Mode 1 (see section 4.2.1 of FRF.8) • **0** or **1**—Specifies Mode 2 (see section 4.2.1 of FRF.8)
de-bit {**0** | **1** | **map-clp**}	(Optional) Sets the mode of DE/CLP mapping in the ATM-to-Frame Relay direction. The default is **map-clp**. • **map-clp**—Specifies Mode 1 (see section 4.2.1 of FRF.8) • **0** or **1**—Specifies Mode 2 (see section 4.2.1 of FRF.8)
efci-bit {**0** | **1** | **map-fecn**}	(Optional) Sets FECN and the ATM EFCI in the Frame Relay-to-ATM direction. **map-fecn** is the default. • **0**—Sets a constant value rather than mapping. • **1**—Sets a constant value rather than mapping. • **map-fecn**—Adheres to Mode 1 and maps the FECN indicators to EFCI indicators.
interface atm0 {*vpi*/*vci* | *vcd*}	Maps the Frame Relay PVC to an ATM PVC specified by slot number (0 is the only option for ATM on the Cisco MC3810) and either one of the following labels: • *vpi*/*vci*—The virtual path identifier-virtual channel identifier (VPI-VCI) pair for the ATM PVC • *vcd*—The ATM virtual circuit descriptor (VCD) for the ATM PVC

Command Default

No Frame Relay PVCs are configured.

Command Modes Interface configuration

Command History

Release	Modification
12.0(7)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 applies only to Frame Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810. Use this command to create Frame Relay PVCs for association with ATM PVCs when you are configuring FRF.8 Frame Relay-ATM Service Interworking on the Cisco MC3810 multiservice access concentrator.

Examples The following example shows two Frame Relay PVCs configured on a serial interface of a Cisco MC3810:

```
frame-relay pvc 222 service translation clp-bit map-de de-bit map-clp efci-bit map-fecn
interface ATM0 222/222
frame-relay pvc 925 service transparent clp-bit map-de de-bit map-clp efci-bit map-fecn
interface ATM0 92/92
```

Related Commands

Command	Description
pvc	Creates an ATM PVC on a main interface or subinterface; assigns a name to an ATM PVC; specifies ILMI, QSAAL, or SMDS as the encapsulation type on an ATM PVC; or enters interface-ATM-VC configuration mode.

frame-relay qos-autosense

Note Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.1(3)T, the **frame-relay qos-autosense** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line.

This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the *Legacy QoS Command Deprecation* feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Note Effective with Cisco IOS XE Release 3.2S, the **frame-relay qos-autosense** command is removed.

To enable Enhanced Local Management Interface (ELMI), use the **frame-relay qos-autosense** command in interface configuration mode. To disable ELMI, use the **no** form of this command.

frame-relay qos-autosense

no frame-relay qos-autosense

Syntax Description

This command has no arguments or keywords.

Command Default

ELMI is disabled.

Command Modes

Interface configuration (config-if)

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.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. Permanent virtual circuits (PVCs) are not provisioned according to the QoS information sent by the router.
15.1(3)T	This command was modified. This command was hidden.
Cisco IOS XE Release 3.2S	This command was removed. It is not available in Cisco IOS XE Release 3.2S and later Cisco IOS XE 3S releases.

Usage Guidelines

ELMI must be configured on both the Cisco router and the Cisco switch.

Examples

The following example shows how to enable a Frame Relay interface to receive ELMI messages from a Cisco switch that is also configured with ELMI enabled.

```
interface serial0
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
  frame-relay qos-autosense

interface serial0.1 point-to-point
  no ip address
  frame-relay interface-dlci 101
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay adaptive-shaping	Selects the type of backward notification you want to use.
show frame-relay qos-autosense	Displays the QoS values sensed from the switch.

frame-relay route

To specify the static route for permanent virtual circuit (PVC) switching, use the **frame-relay route** command in interface configuration mode. To remove a static route, use the **no** form of this command.

frame-relay route *in-dlci* **interface** *out-interface-type out-interface-number out-dlci* [**voice-encap** *size*]

no frame-relay route *in-dlci* **interface** *out-interface-type out-interface-number out-dlci* [**voice-encap** *size*]

Syntax Description

in-dlci	DLCI on which the packet is received on the interface.
interface *out-interface-type out-interface-number*	Interface that the router or access server uses to transmit the packet.
out-dlci	DLCI that the router or access server uses to transmit the packet over the interface specified by the *out-interface* argument.
voice encap *size*	(Optional) (Supported on the Cisco MC3810 only.) Specifies that data segmentation will be used to support Voice over Frame Relay. Note that the voice encapsulation applies only to the input DLCI side. The valid range is from 8 to 1600.

Defaults

No static route is specified.

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

When used with voice, the **frame-relay route** command is applied on both interfaces. If the **voice-encap** keyword is specified on one interface, the incoming frames on that interface are defragmented before being routed to the other interface. The outgoing frames on that interface are then fragmented after being routed from the other interface, and before transmission out the interface.

Note Static routes cannot be configured over tunnel interfaces on the Cisco 800 series, 1600 series, and 1700 series platforms. Static routes can only be configured over tunnel interfaces on platforms that have the Enterprise feature set.

Examples

The following example configures a static route that allows packets in DLCI 100 and sends packets out over DLCI 200 on interface serial 2:

```
frame-relay route 100 interface Serial 2 200
```

The following example illustrates the commands you enter for a complete configuration that includes two static routes for PVC switching between interface serial 1 and interface serial 2:

```
interface Serial1
 no ip address
 encapsulation frame-relay
 keepalive 15
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 100 interface Serial 2 200
 frame-relay route 101 interface Serial 2 201
 clockrate 2000000
```

frame-relay svc

To enable Frame Relay switched virtual circuit (SVC) operation on the specified interface, use the **frame-relay svc** command in interface configuration mode. To disable SVC operation on the specified interface, use the **no** form of this command.

frame-relay svc

no frame-relay svc

Syntax Description

This command has no arguments or keywords.

Defaults

SVC operation is not enabled.

Command Modes

Interface configuration

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

SVC operation can be enabled at the interface level only. Once it is enabled at the interface level, it is enabled on all subinterfaces on the interface. One signaling channel, DLCI 0, is set up for the interface, and all SVCs are controlled from the physical interface.

The first use of this command on the router starts all SVC-related processes on the router. If they are already up and running because SVCs are enabled on another interface, no additional action is taken. These processes are not removed once they are created.

Examples

The following example enables Frame Relay SVC operation on serial interface 0 and starts SVC-related processes on the router:

```
interface serial 0
 ip address 172.68.3.5 255.255.255.0
 encapsulation frame-relay
 frame-relay lmi-type q933a
 frame-relay svc
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay lmi-type	Selects the LMI type.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed bit signalling).
ip address	Sets a primary or secondary IP address for an interface.

frame-relay switching

To enable permanent virtual switching (PVC) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI), use the **frame-relay switching** command in global configuration mode. To disable switching, use the **no** form of this command.

frame-relay switching

no frame-relay switching

Syntax Description

This command has no arguments or keywords.

Defaults

Switching is not enabled.

Command Modes

Global 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

You must add this command to the configuration file before configuring the routes.

Examples

The following example shows the command that is entered in the configuration file before the Frame Relay configuration commands to enable switching:

```
frame-relay switching
```

frame-relay tc

To set the measurement interval for policing incoming traffic when the committed information rate (CIR) is zero, use the **frame-relay tc** command in map-class configuration mode. To reset the measurement interval for policing, use the **no** form of this command.

frame-relay tc *milliseconds*

no frame-relay tc *milliseconds*

Syntax Description

milliseconds	Time interval from 10 ms to 10,000 ms, during which incoming traffic cannot exceed committed burst size (Bc) plus excess burst size (Be).

Defaults

1000 ms

Command Modes

Map-class 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

You must enable Frame Relay policing on the incoming interface, using the **frame-relay policing** interface command, before you can configure traffic-policing parameters.

You must enable Frame Relay switching using the **frame-relay switching** global command before the **frame-relay tc** command will be effective on switched PVCs.

When the CIR is greater than 0, Tc is equal to Bc divided by the CIR.

Examples

The following example shows how to configure a policing measurement interval of 800 milliseconds within a map class called “police”:

```
map-class frame-relay police
 frame-relay tc 800
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay virtual circuit.
frame-relay be	Specifies the incoming or outgoing Be for a Frame Relay virtual circuit.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay virtual circuit.
frame-relay policing	Enables Frame Relay policing on all switched PVCs on an interface.
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.

frame-relay traffic-rate

To configure all the traffic-shaping characteristics of a virtual circuit (VC) in a single command, use the **frame-relay traffic-rate** command in map-class configuration mode. To remove the specified traffic shaping from the map class, use the **no** form of this command.

frame-relay traffic-rate *average* [*peak*]

no frame-relay traffic-rate *average* [*peak*]

Syntax Description

average	Average rate, in bits per second; equivalent to specifying the contracted committed information rate (CIR).
peak	(Optional) Peak rate, in bits per second; equivalent to CIR + Be/Tc = CIR (1 + Be/Bc) = CIR + EIR. If the *peak* value is not configured, the peak rate will default to the configured *average* value.

Defaults

If the peak rate is omitted, the default value used is the average rate configured.

Command Modes

Map-class configuration

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

The configured *peak* and *average* rates are converted to the equivalent CIR, excess burst size (Be), and committed burst size (Bc) values for use by the VC. When the values are translated, the *average* rate is used as the CIR. This value is assumed to be for one second. The generated Bc value is 1/8 the CIR value with an interval of 125 milliseconds.

The Be value is derived from the *peak* rate by subtracting by the *average* rate. The value of the *peak* rate minus *average* rate is assumed to be for one second. The generated Be value is 1/8 the *peak* rate minus the *average* rate with an interval of 125 milliseconds. If the *peak* value is not configured, the peak rate will default to the configured *average* value, and the Be value will equal 0.

For example, entering the **frame-relay traffic-rate 64000 96000** command will result in a CIR of 64000 bps. Assuming 8 intervals of 125 milliseconds, the Bc is 64000/8 or 8000 bits. The Be value is calculated by subtracting 64000 from 96000, so the one-second value is 32000 bits. For each 125-millisecond interval, the Be value is 4000 bits.

Note that the **show frame-relay pvc** command displays Be and Bc values based on an interval of one second. Internally the values being used are based on an interval of 125 milliseconds. The configuration examples below include the **frame-relay traffic-rate** command and corresponding **show frame-relay pvc** command output.

The **frame-relay traffic-rate** command lets you configure all the traffic-shaping characteristics of a virtual circuit in a single command. Using it is simpler than the alternative of entering the three commands **frame-relay cir out**, **frame-relay be out** and **frame-relay bc out**, but offers slightly less flexibility.

Examples

The following example associates a map class with specified data-link connection identifier (DLCI) and then sets a traffic rate for the map class (and thus for the DLCI):

```
interface serial 0
 frame-relay interface-dlci 100
  class fast_vc

map-class frame-relay fast_vc
 frame-relay traffic-rate 64000 96000
```

The following sample output for the **show frame-relay pvc** command is for the PVC configured in the preceding example. Note that the display shows values for Be and Bc that are based on an interval of one second. Internally the values being used are based on an interval of 125 milliseconds, which means that the actual Be value being used is 4000 bits and the actual Bc value being used is 8000 bits.

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0.100

  input pkts 0             output pkts 2314         in bytes 0
  out bytes 748080         dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 2308      out bcast bytes 747792
  pvc create time 1d16h, last time pvc status changed 1d16h
  cir 64000     bc 64000     be 32000     byte limit 5000   interval 125
  mincir 32000     byte increment 1000  Adaptive Shaping none
  pkts 12        bytes 3888      pkts delayed 0         bytes delayed 0
  shaping inactive
  traffic shaping drops 0
  Queueing strategy:fifo
  Output queue 0/40, 0 drop, 0 dequeued
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay VC.
frame-relay be	Sets the incoming or outgoing Be for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.

frame-relay traffic-shaping

To enable both traffic shaping and per-virtual-circuit queueing for all permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) on a Frame Relay interface, use the **frame-relay traffic-shaping** command in interface configuration mode. To disable traffic shaping and per-virtual-circuit queueing, use the **no** form of this command.

frame-relay traffic-shaping

no frame-relay traffic-shaping

Syntax Description

This command has no arguments or keywords.

Defaults

Frame Relay traffic shaping is not enabled.

Command Modes

Interface configuration

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

For virtual circuits (VCs) for which no specific traffic-shaping or queueing parameters are specified, a set of default values are used. The default queueing is performed on a first-come, first-served basis.

The default committed information rate (CIR) of 56K will apply in the following situations:

- When traffic shaping is enabled (by using the **frame-relay traffic-shaping** command), but a map-lass is not assigned to the VC
- When traffic shaping is enabled (by using the **frame-relay traffic-shaping** command) and a map class is assigned to the VC, but traffic-shaping parameters have not been defined in the map-class

Frame Relay traffic shaping is not effective for Layer 2 PVC switching using the **frame-relay route** command.

Examples

The following example enables both traffic shaping and per-virtual circuit queueing:

```
frame-relay traffic-shaping
```

Related Commands

Command	Description
frame-relay class	Associates a map class with an interface or subinterface.
frame-relay custom-queue-list	Specifies a custom queue to be used for the VC queueing associated with a specified map class.
frame-relay priority-group	Assigns a priority queue to VCs associated with a map class.
frame-relay traffic-rate	Configures all the traffic-shaping characteristics of a VC in a single command.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

frame-relay traps-maximum dlci-status-change

To change the maximum number of frDLCIStatusChange traps that Frame Relay generates at linkup or when receiving LMI Full Status messages, use the **frame-relay traps-maximum dlci-status-change** command in interface configuration mode. To disable any limit on the number of traps, use the **no** form of this command.

frame-relay traps-maximum dlci-status-change *traps*

no frame-relay traps-maximum dlci-status-change

Syntax Description

traps	Number of traps.

Command Default

Enabled (and the maximum number of traps is equal to the maximum number of trap events specified for the SNMP server message queue).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(33)CC	This command was introduced.
11.1(33)CV	This command was integrated into Cisco IOS Release 11.1(33)CV.
12.1(8)	This command was integrated into Cisco IOS Release 12.1(8).

Usage Guidelines

You should set the maximum number of traps based on the number of PVCs on the interface as well as on the SNMP server message queue length. A low number on an interface with many PVCs can be reached quickly, which can cause a large number of traps to be dropped. Also, you should set this number smaller than the SNMP server message queue length (which is specified by the **snmp-server queue-length** command, which has a default of 10 traps).

The traps counter for this command is reset when a keepalive message is exchanged on the Frame Relay interface.

Note Frame Relay frDLCIStatusChange traps are not generated when the line status or line protocol status of an interface changes to down.

This command does not restrict traps caused by individual circuit status changes.

Examples

The following example sets a maximum of 256 traps on serial interface 3/3:

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface serial 3/3
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay traps-maximum 256
Router(config-if)# end
```

Related Commands

Command	Description
snmp-server enable traps frame-relay	Enables Frame Relay SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.
snmp-server trap link	Enables linkUp/linkDown SNMP traps, which are compliant with RFC 2233.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

frame-relay vc-bundle

To create a Frame Relay permanent virtual circuit (PVC) bundle (if the bundle does not already exist) and to enter Frame Relay VC-bundle configuration mode, use the **frame-relay vc-bundle** command in interface configuration mode. To remove a Frame Relay PVC bundle, use the **no** form of this command.

frame-relay vc-bundle *vc-bundle-name*

no frame-relay vc-bundle *vc-bundle-name*

Syntax Description

vc-bundle-name	Name of the Frame Relay PVC bundle.

Command Default

A Frame Relay PVC bundle is not created.

Command Modes

Interface 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.
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 create a unique Frame Relay PVC bundle (if one has not already been created using the **frame-relay map** command). You can also use this command to enter Frame Relay VC-bundle configuration mode, so that you can configure PVC bundle attributes and PVC bundle members.

Examples

The following example creates a Frame Relay PVC bundle named MAIN-1:

```
interface serial 0
 frame-relay vc-bundle MAIN-1
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI or Frame Relay PVC bundle that connects to the destination address.

fr-atm connect dlci

To connect a Frame Relay data-link connection identifier (DLCI) to an ATM virtual circuit descriptor for FRF.5 Frame Relay-ATM Interworking (currently available only for the Cisco MC3810), use the **fr-atm connect dlci** interface configuration command. The encapsulation type of the current interface must be Frame Relay or Frame Relay 1490 Internet Engineering Task Force (IETF). To remove the DLCI-to-VCD connection, use the **no** form of this command.

fr-atm connect dlci *dlci atm-interface* [**pvc** *name* | [*vpi/*]*vci*] [**clp-bit** {**map-de** | **0** | **1**}] [**de-bit** {**no-map-clp** | **map-clp**}]

no fr-atm connect dlci *dlci atm-interface* [**pvc** *name* | [*vpi/*]*vci*] [**clp-bit** {**map-de** | **0** | **1**}] [**de-bit** {**no-map-clp** | **map-clp**}]

Syntax Description

dlci	Frame Relay DLCI number.
atm-interface	ATM interface connected to the DLCI.
pvc *name*	(Optional) ATM PVC name.
vpi/*vci*	(Optional) ATM PVC virtual path identifier (VPI)/virtual channel identifier (VCI). The default value for *vpi* is 0 if no value is entered. When specifying the ATM PVC, enter one of the following PVC designations: • The *name* value • The *vpi* value alone • The *vpi/vci* combination
clp-bit {**map-de** | **0** | **1**}	(Optional) Sets the mode of Discard Eligibility/Cell Loss Priority (DE/CLP) mapping in the Frame Relay to ATM direction. The default is **map-de**. **map-de**—Specifies Mode 1 (as described in section 4.4.2 of FRF.5). **0** or **1**—Specifies Mode 2 (as described in section 4.4.2 of FRF.5).
de-bit {**no-map-clp** | **map-clp**}	(Optional) Sets the mode of DE/CLP mapping in the ATM to Frame Relay direction. The default is **map-clp**. **map-clp**—Specifies Mode 1 (as described in section 4.4.2 of FRF.5). **no-map-clp**—Specifies Mode 2 (as described in section 4.4.2 of FRF.5).

Defaults

No Frame Relay-ATM connection is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 MA	This command was introduced.
12.0	Management CLI support was added.
12.0(7)T	The **clp-bit** and **de-bit** keywords 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 only applies to Frame Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810.

Note The Cisco MC3810 provides only *network interworking* (FRF.5). The Cisco MC3810 can be used with *service interworking* (FRF.8), which is provided by the carrier's ATM network equipment.

Examples

The following example configures a Frame Relay-ATM Interworking connection on FR-ATM interface 20, in which Frame Relay DLCI 100 is connected to ATM VPI/VCI 100/200 for ATM interface 0:

```
interface fr-atm 20
 fr-atm connect dlci 100 atm0 100/200 clp-bit map-de de-bit map-clp
```

The following example configures a Frame Relay-ATM Interworking connection on FR-ATM interface 10, in which Frame Relay DLCI 150 is connected to ATM VPI/VCI 0/150 for ATM interface 0:

```
interface fr-atm 10
 fr-atm connect dlci 150 atm0 0/150 clp-bit map-de de-bit map-clp
```

Related Commands

Command	Description
interface fr-atm	Creates a Frame Relay-ATM Interworking interface on the Cisco MC3810 multiservice concentrator.

hello

To configure the interval used to exchange hello keepalive packets in a Layer 2 control channel, use the **hello** command in L2TP class configuration mode. To disable the sending of hello keepalive packets, use the **no** form of this command.

hello *seconds*

no hello *seconds*

Syntax Description

seconds	Number of seconds that a router at one end of a Layer 2 control channel waits between sending hello keepalive packets to its peer router. The valid values range from 0 to 1000 seconds. The default value is 60 seconds.

Command Default

The router sends hello keepalive packets at 60 second intervals.

Command Default

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

You can configure different values with the **hello** command on the router at each end of a Layer 2 control channel.

Examples

The following example sets an interval of 120 seconds between sending of hello keepalive messages in pseudowires that have been configured using the L2TP class configuration named “l2tp class1”:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# hello 120
```

Related Commands

Command	Description
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.

hidden

To hide the attribute-value (AV) pair values in Layer 2 Tunneling Protocol (L2TP) control messages, use the **hidden** command in L2TP class configuration mode. To unhide AV pairs, use the **no** form of this command.

hidden

no hidden

Syntax Description

This command has no arguments or keywords.

Command Default

L2TP AV pair hiding 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.
12.0(29)S	This command was modified to function only with the authentication method configured with the **digest secret** command and keyword combination.
12.2(27)SBC	This command was modified to function only with the authentication method configured with the **digest secret** command and keyword combination.

Usage Guidelines

Use the **hidden** command to provide additional security for the exchange of control messages between provider edge routers in a Layer 2 Tunnel Protocol Version 3 (L2TPv3) control channel. Because username and password information is exchanged between devices in clear text, it is useful to encrypt L2TP AVP values with the **hidden** command.

In Cisco IOS Release 12.0(29)S and Cisco IOS Release 12.2(27)SBC, only the hiding of the cookie AVP is supported.

In Cisco IOS Release 12.0(29)S and Cisco IOS Release 12.2(27)SBC, this command was modified to function only with the authentication method configured using the **digest secret** command and keyword combination. AVP hiding is enabled only when both the **digest secret** command and keyword combination and the **hidden** command have been issued. If another method of authentication is also configured, such as Challenge Handshake Authentication Protocol (CHAP) style authentication configured with the L2TP class command **authentication**, AVP hiding will not be enabled.

If AVP hiding is configured, the session local cookie will be hidden when sent in incoming-call-request (ICRQ) and incoming-call-reply (ICRP) messages.

Whether or not AVP hiding is enabled, if a hidden AVP is received the AVP will be unhidden using the shared secret configured with the **digest secret** command and keyword combination. If no shared secret is configured, the AVP will not be unhidden and an error will be reported. If the M-bit is set in the received hidden AVP, the control channel or tunnel will be torn down.

Examples

The following example enables AVP hiding and encrypts AVPs in control messages in L2TPv3 pseudowires configured using the L2TP class configuration named l2tp class1:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# digest secret cisco hash sha
Router(config-l2tp-class)# hidden
```

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.

hostname (L2TP)

To configure the hostname that the router will use to identify itself during Layer 2 Tunnel Protocol Version 3 (L2TPv3) authentication, use the **hostname** command in L2TP class configuration mode. To remove the hostname, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

name	Name used to identify the router during authentication.

Command Default

No hostname is specified for L2TPv3 authentication.

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

If you do not use the **hostname** command, the hostname of the router is used for L2TPv3 authentication.

Examples

The following example configures the hostname yb2 for a provider edge router used at one end of an L2TPv3 control channel in an L2TPv3 pseudowire that has been configured using the L2TP class configuration named l2tp class1:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# hostname yb2
```

Related Commands

Command	Description
ip local interface	Configures the IP address of the PE router interface to be used as the source IP address for sending tunneled packets.
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.

inarp (Frame Relay VC-bundle-member)

To override the default permanent virtual circuit (PVC) bundle member used for Inverse Address Resolution Protocol (ARP) and specify a different PVC bundle member to handle the Inverse ARP packets, use the **inarp** command in Frame Relay VC-bundle-member configuration mode. To disable Inverse ARP on the PVC bundle member, use the **no** form of this command.

inarp

no inarp

Syntax Description

This command has no arguments or keywords.

Defaults

Inverse ARP is handled by the PVC that handles precedence or EXP level 6 or DSCP level 63.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

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

Usage Guidelines

In each Frame Relay PVC bundle, Inverse ARP by default is handled by the PVC that handles precedence or EXP level 6 or DSCP level 63. In the default case, if the PVC handling Inverse ARP traffic goes down, the Inverse ARP packets are diverted to the PVC that has been configured to handle the bumped traffic for precedence level 6 or DSCP level 63.

Inverse ARP packets arriving on PVCs that are not configured to handle Inverse ARP will be dropped.

If you override the default packet service levels and enable Inverse ARP on a PVC that handles a different precedence or DSCP level, and that PVC goes down, the Inverse ARP packets will be dropped even if another PVC accepts the bumped traffic from the failed PVC.

If the **inarp** command is entered on two different PVC bundle members, Inverse ARP traffic will be handled by the second entry.

Examples

The following example shows Inverse ARP enabled on PVC 250, which handles DSCP level 60:

```
interface serial 1/4.1 multipoint
 frame-relay vc-bundle MP-4-dynamic
  match dscp
  pvc 100
   dscp other
  pvc 250
   dscp 60
   inarp
```

Related Commands

Command	Description
dscp (Frame Relay VC-bundle-member))	Configures the DSCP value or values for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

interface fr-atm

To create a Frame Relay-ATM Interworking interface on the Cisco MC3810 and to enter Frame Relay-ATM Interworking configuration mode, use the **interface fr-atm** command in global configuration mode. To delete the Frame Relay-ATM Interworking interface, use the **no** form of this command.

interface fr-atm *number*

no interface fr-atm *number*

Syntax Description

number	The Frame Relay-ATM Interworking interface number. Range is from 0 to 20.

Defaults

Frame Relay-ATM Interworking interface 20 is configured by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3 MA	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 applies to Frame Relay-ATM Interworking on the Cisco MC3810 only.

Use the **interface fr-atm** command to enter Frame Relay-ATM interworking interface configuration mode. When you issue this command for the first time, an interface number is created dynamically. You can configure up to 21 Frame Relay-ATM interworking interfaces.

Note The Cisco MC3810 provides only *network interworking* (FRF.5). The Cisco MC3810 can be used with *service interworking* (FRF.8), which is provided by the carrier's ATM network equipment.

Examples

The following example configures Frame Relay-ATM Interworking interface number 20:

```
interface fr-atm 20
```

Related Commands

Command	Description
fr-atm connect dlci	Maps a Frame Relay DLCI to an ATM virtual circuit descriptor for FRF.5 Frame Relay-ATM internetworking.

interface mfr

To configure a multilink Frame Relay bundle interface, use the **interface mfr** command in global configuration mode. To remove the bundle interface, use the **no** form of this command.

interface mfr *number*

no interface mfr *number*

Syntax Description

number	Number that will uniquely identify this bundle interface. Range: 0 to 2147483647.

Command Default

A Frame Relay bundle interface is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was introduced on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
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.

Usage Guidelines

Frame Relay encapsulation is the default encapsulation type for multilink Frame Relay bundle interfaces.

A bundle interface is a virtual interface that serves as the Frame Relay data link and performs the same functions as a physical interface. The bundle is made up of physical serial links, called bundle links. The bundle links within a bundle function as one physical link and one pool of bandwidth. Functionality that you want to apply to the bundle links must be configured on the bundle interface.

The **no interface mfr** command will work only if all bundle links have been removed from the bundle by using the **no encapsulation frame-relay mfr** command.

Examples

The following example shows the configuration of a bundle interface called “mfr0.” The bundle identification (BID) name “BUNDLE-A” is assigned to the bundle. Serial interfaces 0 and 1 are assigned to the bundle as bundle links.

```
interface mfr0
 frame-relay multilink bid BUNDLE-A
!
interface serial0
 encapsulation frame-relay mfr0
!
interface serial1
 encapsulation frame-relay mfr0
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

interface serial multipoint

To define a logical subinterface on a serial interface to support multiple logical IP subnetworks over Switched Multimegabit Data Service (SMDS), use the **interface serial multipoint** interface configuration command.

interface serial {*interface* | *slot/port*}**.***subinterface* **multipoint**

Syntax Description

interface	Interface number.
slot/port	Slot and port number related to specified subinterface (for Cisco 7000 and 7500 series routers).
.*subinterface*	Number for this subinterface; values in the range 0 to 255.

Defaults

This command has no default values.

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

Use this command only for routers that need knowledge of multiple IP networks. Other routers can be configured with information only about their own networks. A period must be used to separate the *interface* or *slot/port* from the *subinterface*.

Examples

The following example configures serial interface 2 with multipoint logical subinterface 1:

```
interface serial 2.1 multipoint
```

The following example configures slot 2 port 0 with multipoint logical subinterface 1:

```
interface serial 2/0.1 multipoint
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
smds address	Specifies the SMDS individual address for a particular interface.

Command	Description
smds enable-arp	Enables dynamic ARP.The multicast address for ARP must be set before this command is issued.
smds multicast	Assigns a multicast SMDS E.164 address to a higher-level protocol.

interworking

To enable the L2VPN Interworking feature, use the **interworking** command in pseudowire class configuration mode. To disable the L2VPN Interworking feature, use the **no** form of this command.

interworking {**ethernet** | **ip** | **vlan**}

no interworking {**ethernet** | **ip** | **vlan**}

Syntax Description

ethernet	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, which leaves a pure Ethernet frame.
ip	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.
vlan	Causes Ethernet frames and the VLAN tag to be sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped.

Defaults

L2VPN interworking is not enabled.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(52)SE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
12.2(33)SRE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.

Usage Guidelines

Table 17 shows which L2VPN Interworking features support Ethernet, IP, and VLAN types of interworking.

Table 17 L2VPN Interworking Feature Support

L2VPN Interworking Feature	Interworking Support
Frame Relay to PPP	IP
Frame Relay to ATM AAL5	IP
Ethernet/VLAN to ATM AAL5	IP and Ethernet
Ethernet/VLAN to Frame Relay	IP and Ethernet
Ethernet/VLAN to PPP	IP
Ethernet to VLAN	IP, Ethernet, and VLAN
L2VPN Interworking: VLAN Enable/Disable Option for AToM	Ethernet VLAN

Examples

The following example shows a pseudowire class configuration that enables the L2VPN Interworking feature:

```
pseudowire-class ip-interworking
 encapsulation mpls
 interworking ip
```

Related Commands

Command	Description
encapsulation l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method for tunneling IP traffic over the pseudowire.
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

ip dfbit set

To enable the Don't Fragment (DF) bit in the outer Layer 2 header, use the **ip dfbit set** command in pseudowire class configuration mode. To disable the DF bit setting, use the **no** form of this command.

ip dfbit set

no ip dfbit set

Syntax Description

This command has no arguments or keywords.

Command Default

On the Cisco 10720 Internet router and Cisco 12000 series Internet routers, the DF bit is on (enabled) by default. On other platforms, the DF bit is off (disabled) by default.

Command Modes

Pseudowire 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.
12.0(32)SY	Support was added on the Cisco 10720 Internet router for the L2TPv3 Layer 2 fragmentation feature.

Usage Guidelines

Use this command to set the DF bit on if, for performance reasons, you do not want tunneled packet reassembly to be performed on the router.

Note The **no ip dfbit set** command is not supported on the Cisco 10720 Internet router and Cisco 12000 series Internet routers.

Examples

The following example shows how to enable the DF bit in the outer Layer 2 header in pseudowires that were created from the pseudowire class named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip dfbit set
```

Related Commands

Command	Description
ip pmtu (L2TP)	Enables the discovery of a PMTU for Layer 2 traffic.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip local interface

To configure the IP address of the provider edge (PE) router interface to be used as the source IP address for sending tunneled packets, use the **ip local interface** command in pseudowire class configuration mode. To remove the IP address, use the **no** form of this command.

ip local interface *interface-name*

no ip local interface *interface-name*

Syntax Description

interface-name	Name of the PE interface whose IP address is used as the source IP address for sending tunneled packets over a Layer 2 pseudowire.

Command Default

No IP address is configured.

Command Modes

Pseudowire 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

Use the same local interface name for all pseudowire classes configured between a pair of PE routers. It is highly recommended that you configure a loopback interface with this command. If you do not configure a loopback interface, the router will choose the "best available local address," which could be any IP address configured on a core-facing interface. This configuration could prevent a control channel from being established.

Note The interface configured with the **ip local interface** command must be a loopback interface on Cisco 12000 series Internet routers.

Note This command must be configured for pseudowire class configurations using Layer 2 Tunnel Protocol version 3 (L2TPv3) as the data encapsulation method.

Examples

The following example shows how to configure the IP address of the local Ethernet interface 0/0 as the source IP address for sending Ethernet packets through an L2TPv3 session:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip local interface ethernet 0/0
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip pmtu

To enable the discovery of the path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group, VPDN template, or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

ip pmtu

no ip pmtu

Syntax Description

This command has no arguments or keywords.

Command Default

Path MTU discovery is disabled.

Command Modes

VPDN group configuration (config-vpdn)
VPDN template configuration (config-vpdn-templ)
Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S and support was added for using this command in pseudowire class configuration mode.
12.3(2)T	Support was added for using this command in pseudowire class configuration mode.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.6.2	This command was integrated into Cisco IOS XE Release 2.6.2.

Usage Guidelines

When the **ip pmtu** command is enabled, the Don't Fragment (DF) bit is copied from the inner IP header to the Layer 2 encapsulation header.

Enabling the **ip pmtu** command triggers Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. If an IP packet is larger than the MTU of any interface, it must pass through and the DF bit is set, the packet is dropped and an ICMP unreachable message is returned. The ICMP unreachable message indicates the MTU of the interface that was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission, allowing it to fit through that interface.

Note When path MTU discovery (PMTUD) is enabled, VPDN deployments are vulnerable to Denial of Service (DoS) attacks that use crafted Internet Control Message Protocol (ICMP) “fragmentation needed and Don't Fragment (DF) bit set” (code 4) messages, also known as PMTUD attacks.

Crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. When PMTUD is enabled, it is highly recommended that you use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU to block PMTUD attacks.

Enabling PMTUD will decrease switching performance.

When issued in VPDN group configuration mode, the **ip pmtu** command enables any tunnel associated with the specified virtual private dial-up network (VPDN) group to participate in path MTU discovery.

When issued in VPDN template configuration mode, the **ip pmtu** command enables any tunnel associated with the specified VPDN template to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 Tunnel Protocol Version 3 (L2TPv3) session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Examples

The following example configures a VPDN group named dial-in on a Layer 2 Tunnel Protocol (L2TP) tunnel server and uses the **ip pmtu** command to specify that tunnels associated with this VPDN group will participate in path MTU discovery. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# vpdn-group dial-in
Router(config-vpdn)# request-dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 1
!
Router(config-vpdn)# l2tp security crypto-profile l2tp
Router(config-vpdn)# no l2tp tunnel authentication
Router(config-vpdn)# lcp renegotiation on-mismatch
Router(config-vpdn)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

The following example shows how to enable the discovery of the path MTU for pseudowires that are created from the pseudowire class named ether-pw. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip pmtu
!
Router(config)# vpdn pmtu maximum 1460
Router(config)# vpdn pmtu minimum 576
```

Related Commands

Command	Description
ip dfbit set	Enables the DF bit in the outer L2TPv3 tunnel header.
ip mtu	Sets the MTU size of IP packets sent on an interface.
ip mtu adjust	Enables automatic adjustment of the IP MTU on a virtual access interface.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
vpdn pmtu	Manually configures a range of allowed path MTU sizes for an L2TP VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

ip protocol

To configure the Layer 2 Tunnel Protocol (L2TP) or Universal Tunnel Interface (UTI) as the IP protocol used for tunneling packets in a Layer 2 pseudowire, use the **ip protocol** command in pseudowire class configuration mode. To remove the IP protocol configuration, use the **no** form of this command.

ip protocol {**l2tp** | **uti** | *protocol-number*}

no ip protocol {**l2tp** | **uti** | *protocol-number*}

Syntax Description

l2tp	Configures L2TP as the IP protocol used to tunnel packets in a Layer 2 pseudowire. This is the default.
uti	Configures UTI as the IP protocol used to tunnel packets in a Layer 2 pseudowire, and allows a router running L2TP version 3 (L2TPv3) to interoperate with a peer running UTI.
protocol-number	The protocol number of the desired IP protocol. The protocol number for L2TPv3 is 115. The protocol number for UTI is 120.

Command Default

The default IP protocol is L2TP.

Command Modes

Pseudowire 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

Use the **ip protocol** command to ensure backward compatibility with routers running UTI. This command allows you to configure an L2TPv3 pseudowire between a router running L2TPv3 and a peer router running UTI.

Note You can use the **ip protocol** command only if you have already entered the **encapsulation l2tpv3** command.

To configure L2TP as the IP protocol that is used to tunnel packets in an L2TPv3 pseudowire, you may enter **115**, the IP protocol number assigned to L2TPv3, instead of **l2tp** in the **ip protocol** command.

To configure UTI as the IP protocol that is used to tunnel packets in an L2TPv3 pseudowire, you may enter **120**, the IP protocol number assigned to UTI, instead of **uti** in the **ip protocol** command.

Note Interoperability in an L2TPv3 control channel between a router running UTI and a router configured for L2TPv3 encapsulation is supported only if you disable signaling using the **protocol none** command.

Examples

The following example shows how to configure UTI as the IP protocol used to tunnel packets in an L2TPv3 pseudowire created from the pseudowire class named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation l2tpv3
Router(config-pw)# ip protocol uti
```

Related Commands

Command	Description
encapsulation (L2TP)	Configures the Layer 2 data encapsulation method used to tunnel IP traffic.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session, and that control plane configuration settings are to be taken from a specified L2TP class.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip tos (L2TP)

To configure the Type of Service (ToS) byte in the header of Layer 2 tunneled packets, use the **ip tos** command in pseudowire class configuration mode. To disable a configured ToS value or IP ToS reflection, use the **no** form of this command.

ip tos {**value** *value* | **reflect**}

no ip tos {**value** *value* | **reflect**}

Syntax Description

value *value*	Sets the value of the ToS byte for IP packets in a Layer 2 Tunnel Protocol version 3 (L2TPv3) session. Valid values range from 0 to 255. The default value is 0.
reflect	Sets the value of the ToS byte for IP packets in an L2TPv3 session to be reflected from the inner IP header.

Command Default

The default ToS value is 0.

Command Modes

Pseudowire 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

The **ip tos** command allows you to manually configure the value of the ToS byte used in the headers of Layer 2 tunneled packets or to have the ToS value reflected from the IP header of the encapsulated packet.

Note The **reflect** option is not supported on the Cisco 10720 and Cisco 12000 series Internet routers.

Note IP ToS byte reflection functions only if traffic in an L2TPv3 session carries IP packets as its payload.

In addition, you can configure both IP ToS reflection and a ToS priority level (from 0 to 255) for a pseudowire class. In this case, the ToS value in the tunnel header defaults to the value you specify with the **ip tos value** *value* command. IP packets received on the Layer 2 interface and encapsulated into the L2TPv3 session have their ToS byte reflected into the outer IP session, overriding the default value configured with the **ip tos value** *value* command.

Examples

In the following example, the ToS byte in the headers of tunneled packets in Layer 2 tunnels created from the pseudowire class named “ether-pw” will be reflected from the ToS value in the header of each encapsulated IP packet:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip tos reflect
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip ttl

To configure the time-to-live (TTL) byte in the IP headers of Layer 2 tunneled packets, use the **ip ttl** command in pseudowire class configuration mode. To remove the configured TTL value, use the **no** form of this command.

ip ttl *value*

no ip ttl value

Syntax Description

value	Value of the TTL byte in the IP headers of L2TPv3 tunneled packets. The valid values range from 1 to 255. The default value is 255.

Command Default

The default value of the TTL byte is 255.

Command Modes

Pseudowire 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

Use this command to set the Don't Fragment (DF) bit on if, for performance reasons, you do not want tunneled packet reassembly to be performed on the router.

Examples

The following example shows how to set the TTL byte to 100 in the IP header of Layer 2 tunneled packets in pseudowires that were created from the pseudowire class named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip ttl 100
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

keepalive (LMI)

To enable the Local Management Interface (LMI) mechanism for serial lines using Frame Relay encapsulation, use the **keepalive** command in interface configuration mode. To disable this capability, use the **no** form of this command.

keepalive *number*

no keepalive

Syntax Description

number	Number of seconds that defines the keepalive interval. The interval must be set as a positive integer that is less than the interval set on the switch; see the **frame-relay lmi-t392dce** command description earlier in this chapter.

Defaults

10 seconds

Command Modes

Interface configuration

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

The **keepalive** command enables the keepalive sequence, which is part of the LMI protocol.

Note When booting from a network server over Frame Relay, you might need to disable keepalives.

Examples

The following example sets the keepalive timer on the server for a period that is two or three seconds faster (has a shorter interval) than the interval set on the keepalive timer of the Frame Relay switch. The difference in keepalive intervals ensures proper synchronization between the Cisco server and the Frame Relay switch.

```
interface serial 3
 keepalive 8
```

Related Commands

Command	Description
frame-relay lmi-t392dce	Sets the polling verification timer on a DCE or NNI interface.

l2 router-id

To specify a router ID for the provider edge (PE) router to use with Virtual Private LAN Services (VPLS) Autodiscovery pseudowires, use the **l2 router-id** command in L2 VFI configuration mode. To revert to the MPLS global router ID, use the **no** form of this command.

l2 router-id *ip-address*

no l2 router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Defaults

The Layer 2 router ID is set to the Multiprotocol Label Switching (MPLS) global router ID.

Command Modes

L2 VFI configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

The Layer 2 router ID is used in the forward equivalence class (FEC) 129 encoding for pseudowire signaling It is also used in the network layer reachability information (NLRI) for peer discovery.

Examples

The following example specifies a Layer 2 router ID:

```
l2 router-id 10.1.1.1
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

l2 vfi autodiscovery

To enable the Virtual Private LAN Service (VPLS) provider edge (PE) router to automatically discover other PE routers that are part of the same VPLS domain, use the **l2 vfi autodiscovery** command in global configuration mode. To disable VPLS autodiscovery, use the **no** form of this command.

l2 vfi *vfi-name* **autodiscovery**

no l2 vfi *vfi-name* **autodiscovery**

Syntax Description

vfi-name	Specifies the name of the virtual forwarding instance. The virtual forwarding instance (VFI) identifies a group of pseudowires that are associated with a virtual switching instance (VSI).

Command Default

Layer 2 VFI autodiscovery is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

VPLS Autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. Beginning with Cisco IOS Release 12.2(33)SRB, you no longer need to manually configure the VPLS neighbors and maintain the configuration when a PE router is added or deleted. However, you can still perform manual VPLS configuration even when you enable VPLS Autodiscovery.

Examples

The following example enables VPLS Autodiscovery on a PE router:

```
l2 vfi vfi2 autodiscovery
```

Related Commands

Command	Description
l2 vfi manual	Manually creates a Layer 2 VFI.

l2tp cookie local

To configure the size of the cookie field used in the Layer 2 Tunnel Protocol Version 3 (L2TPv3) headers of incoming packets received from the remote provider edge (PE) peer router, use the **l2tp cookie local** command in xconnect configuration mode. To remove the configured cookie field parameters, use the **no** form of this command.

l2tp cookie local *size low-value* [*high-value*]

no l2tp cookie local *size low-value* [*high-value*]

Syntax Description

size	The size of the cookie field in L2TPv3 headers. The valid values are 0, 4, and 8.
low-value	The value of the lower 4 bytes of the cookie field.
high-value	(Optional) The value of the upper 4 bytes of the cookie field. For 8-byte cookie fields, you must enter the value for the upper 4 bytes of the cookie field.

Command Default

No cookie value is included in the header of L2TP packets.

Command Modes

Xconnect configuration (config-if-xconn)

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	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **l2tp cookie local** command specifies the values that the peer PE router includes in the cookie field in L2TPv3 headers of the packets it sends to the local PE router through an L2TPv3 session. These values are required in a static L2TPv3 session.

The cookie field is an optional part of an L2TPv3 header with a length of either 4 or 8 bytes. If you specify an 8-byte length, you must also enter a value for the *high-value* argument.

Note For the Cisco 10720 and Cisco 12000 series Internet routers, an 8-byte cookie must be configured with this command.

Examples

The following example shows how to configure the cookie field of 4 bytes starting at 54321 for the L2TPv3 headers in incoming tunneled packets that were sent from the remote PE peer:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp cookie local 4 54321
```

Related Commands

Command	Description
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (sent) packets from the remote PE peer router.
l2tp hello	Configures the interval between hello keepalive messages.
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp cookie remote

To configure the size of the cookie field used in the Layer 2 Tunnel Protocol Version 3 (L2TPv3) headers of outgoing packets sent from the local provider edge (PE) peer router, use the **l2tp cookie remote** command in xconnect configuration mode. To remove the configured cookie field parameters, use the **no** form of this command.

l2tp cookie remote *size low-value* [*high-value*]

no l2tp cookie remote *size low-value* [*high-value*]

Syntax Description

size	The size of the cookie field in L2TPv3 headers. The valid values are 0, 4, and 8.
low-value	The value of the lower 4 bytes of the cookie field.
high-value	(Optional) The value of the upper 4 bytes of the cookie field. For 8-byte cookie fields, you must enter the value for the upper 4 bytes of the cookie field.

Command Default

No cookie value is included in the header of L2TP packets.

Command Modes

Xconnect configuration (config-if-xconn)

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	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **l2tp cookie remote** command specifies the values that the local PE router includes in the cookie field in L2TPv3 headers of the packets it sends to the remote PE router through an L2TPv3 session. These values are required in a static L2TPv3 session.

The cookie field is an optional part of an L2TPv3 header with a length of either 4 or 8 bytes. If you specify an 8-byte length, you must also enter a value for the *high-value* argument.

Examples

The following example shows how to configure the cookie field of 4 bytes starting at 12345 for the L2TPv3 headers in outgoing tunneled packets sent to the remote PE peer:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp cookie remote 4 12345
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp hello	Configures the interval between hello keepalive messages.
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp hello

To specify the use of a hello keepalive setting contained in a specified Layer 2 Tunneling Protocol class configuration for a static Layer 2 Tunnel Protocol Version 3 (L2TPv3) session, use the **l2tp hello** command in xconnect configuration mode. To disable the sending of hello keepalive messages, use the **no** form of this command.

l2tp hello *l2tp-class-name*

no l2tp hello *l2tp-class-name*

Syntax Description

l2tp-class-name	Specifies the L2TP class configuration in which the hello keepalive interval to be used for the L2TPv3 session is stored.

Command Default

No hello keepalive messages are sent.

Command Modes

Xconnect configuration (config-if-xconn)

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

Usage Guidelines

Because a static L2TPv3 session does not use a control plane to dynamically negotiate control channel parameters, you must use the **l2tp hello** command to specify an L2TP class configuration that contains the interval for sending hello keepalive messages.

Examples

The following example shows how to configure the time interval for hello keepalive messages stored in the L2TP class configuration named l2tp-default for an Ethernet interface using the configuration settings stored in the pseudowire class named ether-pw:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp hello lt2p-defaults
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (transmitted) packets from the remote PE peer router.
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp id

To configure the identifiers used by the local and remote provider edge (PE) routers at each end of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) session, use the **l2tp id** command in xconnect configuration mode. To remove the configured identifiers for local and remote sessions, use the **no** form of this command.

l2tp id *local-session-id remote-session-id*

no l2tp id *local-session-ID remote-session-ID*

Syntax Description

local-session-id	The identifier used by the local PE router as its local session identifier.
remote-session-id	The identifier used by the remote PE router as its local session identifier.

Command Default

No session identifiers are configured.

Command Modes

Xconnect configuration (config-if-xconn)

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

Usage Guidelines

The xconnect configuration that binds an attachment circuit to an L2TPv3 pseudowire is not complete without configured values for the *local-session-id* and *remote-session-id* arguments.

Examples

The following example shows how to configure the identifiers named 222 for the local PE router and 111 for the remote peer in an L2TPv3 session bound to an Ethernet circuit using the L2TPv3 configuration settings stored in the pseudowire class names ether-pw:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp id 222 111
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (transmitted) packets from the remote PE peer router.
l2tp hello	Configures the interval between hello keepalive messages.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp-class

To create a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings, which can be inherited by different pseudowire classes, and to enter L2TP class configuration mode, use the **l2tp-class** command in global configuration mode. To remove a specific L2TP class configuration, use the **no** form of this command.

l2tp-class [*l2tp-class-name*]

no l2tp-class *l2tp-class-name*

Syntax Description

l2tp-class-name	(Optional) Name of the L2TP class. The *name* argument must be specified if you want to configure multiple sets of L2TP control parameters.

Command Default

No L2TP classes are defined.

Command Modes

Global configuration (config)

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	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SCC	This command was integrated into Cisco IOS Release12.2(33)SCC.
12.2(50)SQ	This command was integrated into Cisco IOS Release 12.2(50)SQ.

Usage Guidelines

The **l2tp-class** *l2tp-class-name* command lets you configure an L2TP class template that consists of configuration settings used by different pseudowire classes. An L2TP class includes the following configuration settings:

- Hostname of local router used during Layer 2 authentication
- Authentication enabled
- Time interval used for exchange of hello packets
- Password used for control channel authentication
- Packet size of receive window
- Retransmission settings for control packets
- Time allowed to set up a control channel

The **l2tp-class** command enters L2TP class configuration mode, where L2TP control plane parameters are configured.

You must use the same L2TP class in the pseudowire configuration at both ends of a Layer 2 control channel.

Note For Cisco IOS Release 12.2(33)SCC and Cisco IOS Release 12.2(50)SQ, the commands listed under the Related Commands section are not valid.

Examples

The following example shows how to enter L2TP class configuration mode to create an L2TP class configuration template for a class named ether-pw:

```
Router(config)# l2tp-class ether-pw
Router(config-l2tp-class)#
```

Related Commands

Command	Description
protocol (L2TP)	Specifies the Layer 2 signaling protocol to be used to manage the pseudowires created from a pseudowire class for a dynamic Layer 2 session, and that control plane configuration settings are to be taken from the specified L2TP class
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
pseudowire-class	Specifies the name of an L2TP pseudowire class, and enters pseudowire class configuration mode.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service, and enters xconnect configuration mode.

lapb interface-outage

To specify the period for which a link will remain connected, even if a brief hardware outage occurs (partial Link Access Procedure, Balanced [LAPB] T3 timer functionality), use the **lapb interface-outage** interface configuration command.

lapb interface-outage *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) a hardware outage can last without the protocol disconnecting the service.

Defaults

0 ms, which disables this feature.

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

If a hardware outage lasts longer than the LAPB hardware outage period you select, normal protocol operations will occur. The link will be declared down, and when it is restored, a link setup will be initiated.

Examples

The following example sets the interface outage period to 100 ms. The link remains connected for outages equal to or shorter than that period.

```
encapsulation lapb dte ip
lapb interface-outage 100
```

Related Commands

Command	Description
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb k

To specify the maximum permissible number of outstanding frames, called the *window size*, use the **lapb k** interface configuration command.

lapb k *window-size*

Syntax Description

window-size	Frame count. Range: 1 to the modulo size minus 1 (the maximum is 7 if the modulo size is 8; it is 127 if the modulo size is 128).

Defaults

7 frames

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

If the window size is changed while the protocol is up, the new value takes effect only when the protocol is reset. You will be informed that the new value will not take effect immediately.

When using the Link Access Procedure, Balanced (LAPB) modulo 128 mode (extended mode), you must increase the window parameter k to send a larger number of frames before acknowledgment is required. This increase is the basis for the router's ability to achieve greater throughput on high-speed links that have a low error rate.

This configured value must match the value configured in the peer X.25 switch. Nonmatching values will cause repeated LAPB reject (REJ) frames.

Examples

The following example sets the LAPB window size (the k parameter) to 10 frames:

```
interface serial 0
 lapb modulo
 lapb k 10
```

Related Commands

Command	Description
lapb modulo	Specifies the LAPB basic (modulo 8) or extended (modulo 128) protocol mode.

lapb modulo

To specify the Link Access Procedure, Balanced (LAPB) basic (modulo 8) or extended (modulo 128) protocol mode, use the **lapb modulo** interface configuration command.

lapb modulo *modulus*

Syntax Description

modulus	Either 8 or 128. The value 8 specifies LAPB's basic mode; the value 128 specifies LAPB's extended mode.

Defaults

Modulo 8

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

The modulo parameter determines which of LAPB's two modes is to be used. The modulo values derive from the fact that basic mode numbers information frames between 0 and 7, whereas extended mode numbers them between 0 and 127. Basic mode is widely available and is sufficient for most links. Extended mode is an optional LAPB feature that may achieve greater throughput on high-speed links that have a low error rate.

The LAPB operating mode may be set on X.25 links as well as LAPB links. The X.25 modulo is independent of the LAPB layer modulo. Both ends of a link must use the same LAPB mode.

When using modulo 128 mode, you must increase the window parameter k to send a larger number of frames before acknowledgment is required. This increase is the basis for the router's ability to achieve greater throughput on high-speed links that have a low error rate.

If the modulo value is changed while the protocol is up, the new value takes effect only when the protocol is reset. You will be informed that the new value will not take effect immediately.

Examples

The following example configures a high-speed X.25 link to use LAPB's extended mode:

```
interface serial 1
 encapsulation x25
 lapb modulo 128
 lapb k 40
 clock rate 2000000
```

Related Commands

Command	Description
lapb k	Specifies the maximum permissible number of outstanding frames, called the window size.

lapb n1

To specify the maximum number of bits a frame can hold (the Link Access Procedure, Balanced [LAPB] N1 parameter), use the **lapb n1** interface configuration command.

lapb n1 *bits*

Syntax Description

bits	Maximum number of bits in multiples of eight. The minimum and maximum range is dynamically set. Use the question mark (**?**) to view the range.

Defaults

The largest (maximum) value available for the particular interface is the default. The Cisco IOS software dynamically calculates N1 whenever you change the maximum transmission unit (MTU), the L2/L3 modulo, or compression on a LAPB interface.

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

The Cisco IOS software uses the following formula to determine the minimum N1 value:

*(128 (default packet size) + LAPB overhead + X.25 overhead + 2 bytes of CRC) * 8*

The Cisco IOS software uses the following formula to determine for the maximum N1 value:

*(hardware MTU + LAPB overhead + X.25 overhead + 2 bytes of CRC) * 8*

LAPB overhead is 2 bytes for modulo 8 and 3 bytes for modulo 128.

X.25 overhead is 3 bytes for modulo 8 and 4 bytes for modulo 128.

You need not set N1 to an exact value to support a particular X.25 data packet size. The N1 parameter prevents the processing of any huge frames that result from a “jabbering” interface, an unlikely event.

In addition, the various standards bodies specify that N1 be given in bits rather than bytes. While some equipment can be configured in bytes or will automatically adjust for some of the overhead information present, Cisco devices are configured using the true value, in bits, of N1.

You cannot set the N1 parameter to a value less than that required to support an X.25 data packet size of 128 bytes. All X.25 implementations must be able to support 128-byte data packets. Moreover, if you configure N1 to be less than 2104 bits, you receive a warning message that X.25 might have problems because some nondata packets can use up to 259 bytes.

You cannot set the N1 parameter to a value larger than the default unless the hardware MTU size is first increased.

The X.25 software accepts default packet sizes and calls that specify maximum packet sizes greater than those the LAPB layer supports, but negotiates the calls placed on the interface to the largest value that can be supported. For switched calls, the packet size negotiation takes place end-to-end through the router so the call will not have a maximum packet size that exceeds the capability of either of the two interfaces involved.

Caution The LAPB N1 parameter provides little benefit beyond the interface MTU and can easily cause link failures if misconfigured. Cisco recommends that this parameter be left at its default value.

Examples

The following example shows how to use the question mark (**?**) command to display the minimum and maximum N1 value. In this example, X.25 encapsulation has both the LAPB and X.25 modulo set to 8. Any violation of this N1 range results in an "Invalid input" error message.

```
router(config)# interface serial 1
router(config-if)# lapb n1 ?

<1080-12056> LAPB N1 parameter (bits; multiple of 8)
```

The following example sets the N1 bits to 16440:

```
router(config)# interface serial 0
router(config-if)# lapb n1 16440
router(config-if)# mtu 2048
```

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.
mtu	Adjusts the maximum packet size or MTU size.

lapb n2

To specify the maximum number of times a data frame can be sent (the Link Access Procedure, Balanced [LAPB] N2 parameter), use the **lapb n2** interface configuration command.

lapb n2 *tries*

Syntax Description

tries	Transmission count. Range: 1 to 255.

Defaults

20 transmissions

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.

Examples

The following example sets the N2 tries to 50:

```
interface serial 0
 lapb n2 50
```

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb protocol

The **lapb protocol** command has been replaced by the [*protocol* | **multi**] option of the **encapsulation lapb** command. See the description of the [*protocol* | **multi**] option of the **encapsulation lapb** command earlier in this chapter for more information.

lapb t1

To set the retransmission timer period (the Link Access Procedure, Balanced [LAPB] T1 parameter), use the **lapb t1** interface configuration command.

lapb t1 *milliseconds*

Syntax Description

milliseconds	Time in milliseconds. Range: 1 to 64000.

Defaults

3000 ms

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

The retransmission timer determines how long a transmitted frame can remain unacknowledged before the LAPB software polls for an acknowledgment. The design of the LAPB protocol specifies that a frame is presumed to be lost if it is not acknowledged within T1; a T1 value that is too small may result in duplicated control information, which can severely disrupt service.

To determine an optimal value for the retransmission timer, use the **ping** privileged EXEC command to measure the round-trip time of a maximum-sized frame on the link. Multiply this time by a safety factor that takes into account the speed of the link, the link quality, and the distance. A typical safety factor is 1.5. Choosing a larger safety factor can result in slower data transfer if the line is noisy. However, this disadvantage is minor compared to the excessive retransmissions and effective bandwidth reduction caused by a timer setting that is too small.

Examples

The following example sets the T1 retransmission timer to 2000 ms:

```
interface serial 0
 lapb t1 2000
```

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb t2

To set the explicit acknowledge deferral timer (the Link Access Procedure, Balanced [LAPB] T2 parameter), use the **lapb t2** interface configuration command.

lapb t2 *milliseconds*

Syntax Description

milliseconds	Time in milliseconds. Range: 1 to 32000. Default is 0 ms (disabled) and the recommended setting.

Defaults

0 ms (disabled), which means that the software will send an acknowledgement as quickly as possible.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	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

The explicit acknowledge deferral timer determines the time that the software waits before sending an explicit acknowledgement. The acknowledgement is piggybacked with the data, unless there is no data and then an explicit acknowledgement is sent when the timer expires.

Caution It is usually not necessary (or recommended) to set the LAPB T2 timer, but if there is a requirement, it must be set to a value smaller than that set for the LAPB T1 timer; see the ITU X.25 specifications for details.

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb t4

To set the T4 idle timer, after which the Cisco IOS software sends out a Poll packet to determine whether the link has suffered an unsignaled failure, use the **lapb t4** interface configuration command.

lapb t4 *seconds*

Syntax Description

seconds	Number of seconds between receipt of the last frame and transmission of the outgoing poll.

Defaults

0 seconds

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

Any non-zero T4 duration must be greater than T1, the Link Access Procedure, Balanced (LAPB) retransmission timer period.

Examples

The following example will poll the other end of an active link if it has been 10 seconds since the last frame was received. If the far host has failed, the service will be declared down after **n2** tries are timed out.

```
interface serial0
 encapsulation x25
 lapb t4 10
```

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).

Command	Description
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

logging event frame-relay x25

To enable notification of X.25 Annex G session status changes to be displayed on a console or system log, use the **logging event frame-relay x25** command in interface configuration mode. To disable notification, use the **no** form of this command.

logging event frame-relay x25

no logging event frame-relay x25

Syntax Description

This command has no arguments or keywords.

Defaults

X.25 Annex G session status change notifications are not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Examples

The following example shows how to enable notification of X.25 Annex G session status changes to be displayed on a console or system log using the **logging event frame-relay x25** interface configuration command:

```
Router(config-if)# logging event frame-relay x25
```

The following is an example of the Annex G status change notifications:

```
%X25-5-UPDOWN: Interface <interface> - DLCI <dlci number> X.25 packet layer changed state
to DOWN
%X25-5-UPDOWN: Interface <interface> - DLCI <dlci number> X25 packet layer changed state
to UP
```

lz entropy-check

To enable adaptive Lempel-Ziv (LZ) compression through entropy checking, use the **lz entropy-check** command in parameter-map configuration mode. To disable the LZ entropy checking, use the **no** form of this command.

lz entropy-check

no lz entropy-check

Syntax Description

This command has no arguments or keywords.

Command Default

Entropy checking is disabled.

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 enable adaptive LZ compression through entropy checking.

Examples

The following example shows how to enable LZ entropy checking:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile) lz entropy-check
```

Related Commands

Command	Description
cpu-threshold	Sets the CPU threshold limit.
parameter-map type waas	Defines a WAAS Express parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery blacklist	Configures black list with autodiscovery for WAAS Express.
tfo optimize	Configures compression for WAAS Express.

mace enable

To apply the global Measurement, Aggregation, and Correlation Engine (MACE) policy on an interface, use the **mace enable** command in interface configuration mode. To disable the MACE policy on an interface, use the **no** form of this command.

mace enable

no mace enable

Syntax Description

This command has no arguments or keywords.

Command Default

No MACE policy is applied on the interface.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **mace enable** command to apply the global MACE policy on an interface. This command applies the global MACE policy in both directions, ingress and egress, of the interface. The MACE runs on the traffic coming over this interface. MACE policy is limited to those targets for which the Wide Area Application Services (WAAS) policy can be enabled. MACE supports all the interfaces that are supported by WAAS.

To enable MACE, you must first perform the following configurations:

- Flow record of type MACE
- Flow exporter
- Flow monitor of type MACE
- Class map of type WAAS
- Policy map of type MACE

When you configure a **mace enable** command, the metrics of the matching flows are collected and updated on every packet. When the export timer expires, these metrics are aggregated and exported to various collectors, according to the defined configuration. If the flow is optimized by WAAS, the metrics of both segments, pre-WAAS and post-WAAS, of the flow are exported.

Examples

The following example shows how to enable MACE on Ethernet interface 0/0:

```
Router(config)# interface ethernet0/0
Router(config-if)# mace enable
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
flow exporter	Creates a Flexible NetFlow flow exporter.
flow monitor type mace	Configures a flow monitor for MACE.
flow record type mace	Configures a flow record for MACE.
policy-map type mace	Configures a MACE policy map.

mace monitor waas

To enable the Measurement, Aggregation, and Correlation Engine (MACE) monitoring on Wide Area Application Services (WAAS), use the **mace monitor waas** command in global configuration mode. To disable MACE monitoring, use the **no** form of this command.

mace monitor waas [**all** | **optimized**] [**name**] *monitor-name*

no mace monitor waas [**all** | **optimized**] [**name**] *monitor-name*

Syntax Description

all	(Optional) Enables MACE monitoring for all WAAS flows.
optimized	(Optional) Enables MACE monitoring for WAAS-optimized flows.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	Name of the specific flow monitor that is configured using the **flow monitor type mace** command.

Command Default

No MACE is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **mace monitor waas** command to enable MACE for all WAAS instances that run on the router.

MACE monitors all the flows on which WAAS is active for optimization.

To enable MACE on WAAS, you must first configure the following:

- A flow record of type MACE
- A flow exporter
- A flow monitor of type MACE

When you use the **mace monitor waas** command along with the **optimized** keyword, MACE monitors all the flows on which WAAS is active for optimization.

When you use this command along with the **all** keyword, MACE monitors all the flows configured in a WAAS policy. This includes the flows that are subject to either WAAS optimization or pass-through actions.

When you use this command without the **all** or **optimized** keyword, MACE monitors all WAAS classes that have the **optimize** keyword configured in them. MACE also exports the flows that are tagged by WAAS as passthrough, even when they match the classes with optimize actions in them.

Note If you wish to choose a subset of WAAS classes, you must create a global MACE policy that includes the desired classes.

Examples

The following example shows how to configure MACE to monitor all the flows that are configured in a WAAS policy:

```
Router(config)# mace monitor waas all my-flow-monitor
```

Related Commands

Command	Description
flow exporter	Creates a Flexible NetFlow flow exporter.
flow monitor type mace	Configures a flow monitor for MACE.
flow record type mace	Configures a flow record for MACE.
mace enable	Applies the global MACE policy on an interface.

map-class frame-relay

To specify a map class to define quality of service (QoS) values for a virtual circuit (VC), use the **map-class frame-relay** command in global configuration mode. To remove a map class, use the **no** form of this command.

map-class frame-relay *map-class-name*

no map-class frame-relay *map-class-name*

Syntax Description

map-class-name	Name of map class.

Defaults

A map class is not specified.

Command Modes

Global configuration

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

After you specify the named map class, you can specify the QoS parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the map class.

To specify the protocol-and-address combination to which the QoS parameters are to be applied, associate this map class with the static maps under a map list.

Examples

The following example specifies a map class “hawaii” and defines three QoS parameters for it. The “hawaii” map class is associated with a protocol-and-address static map defined under the **map-list** command.

```
map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.108.177.100 class hawaii
 appletalk 1000.2 class hawaii

map-class frame-relay hawaii
 frame-relay cir in 2000000
 frame-relay cir out 56000
 frame-relay be out 9000
```

Related Commands

Command	Description
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay VC.
frame-relay be	Sets the incoming or outgoing Be for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.
frame-relay idle-timer	Specifies the idle timeout interval for an SVC.

map-group

To associate a map list with a specific interface, use the **map-group** command in interface configuration mode.

map-group *group-name*

Syntax Description

group-name	Name used in a **map-list** command.

Defaults

A map list is not associated with an interface.

Command Modes

Interface configuration

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

A map-group association with an interface is required for switched virtual circuit (SVC) operation. In addition, a map list must be configured.

The **map-group** command applies to the interface or subinterface on which it is configured. The associated E.164 or X.121 address is defined by the **map-list** command, and the associated protocol addresses are defined by using the **class** command under the **map-list** command.

Examples

The following example configures a physical interface, applies a map group to the physical interface, and then defines the map group:

```
interface serial 0
 ip address 172.10.8.6
 encapsulation frame-relay
 map-group bermuda
 frame-relay lmi-type q933a
 frame-relay svc

map-list bermuda source-addr E164 123456 dest-addr E164 654321
 ip 10.1.1.1 class hawaii
 appletalk 1000.2 class rainbow
```

Related Commands

Command	Description
class (map-list)	Associates a map class with a protocol-and-address combination.
map-list	Specifies a map group and link 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.

map-list

To specify a map group or map list and link it to a local E.164 or X.121 source address and a remote E.164 or X.121 destination address for Frame Relay switched virtual circuits (SVCs), use the **map-list** command in global configuration mode. To delete a previous map-group link, use the **no** form of this command.

map-list *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**} *destination-address* **clps** *number* [**cdps** *number*]

no map-list *map-group-name* **source-addr** {**e164** | **x121**} *source-address* **dest-addr** {**e164** | **x121**} *destination-address* **clps** *number* [**cdps** *number*]

Syntax Description

map-group-name	Name of the map group or map list. This map group or list must be associated with a physical interface.
source-addr {**e164** | **x121**}	Specifies the type of source address.
source-address	Address of the type specified (E.164 or X.121).
dest-addr {**e164** | **x121**}	Specifies the type of destination address.
destination-address	Address of the type specified (E.164 or X.121).
clps *number*	Specifies the calling party subaddress. The subaddress range is from 1 to 9.
cdps *number*	(Optional) Specifies the called party subaddress. The subaddress range is from 1 to 9.

Defaults

A map group or map list is not linked to a source and destination address.

Command Modes

Global configuration (config)

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.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **clps** *number* and **cdps** *number* keyword and argument pairs were added.

Usage Guidelines

Use the **map-class** command to define quality of service (QoS) parameters—such as incoming and outgoing committed information rate (CIR), committed burst rate, excess burst rate, and the idle timer—for the static maps defined under a map list or map group.

Each SVC needs to use a source and destination number, in much the same way that a public telephone network needs to use source and destination numbers. These numbers allow the network to route calls from a specific source to a specific destination. This specification is done through map lists or map groups.

Depending on switch configuration, addressing can take either of two forms: E.164 or X.121.

An X.121 address number is 14 digits long and has the following form:

```
Z CC P NNNNNNNNNN
```

Table 18 describes the codes in an X.121 address number form.

Table 18 X.121 Address Numbers

Code	Meaning	Value
Z	Zone code	3 for North America
C	Country code	10–16 for the United States
P	Public data network (PDN) code	Provided by the PDN
N	10-digit number	Set by the network for the specific destination

An E.164 number has a variable length; the maximum length is 15 digits. An E.164 number has the fields shown in Figure 1 and described in Table 19.

Figure 1 E.164 Address Format

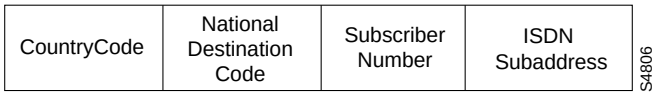

Table 19 E.164 Address Field Descriptions

Field	Description
Country code	Can be 1, 2, or 3 digits long. Some current values are the following: • Code 1—United States of America • Code 44—United Kingdom • Code 61—Australia
National destination code + subscriber number	Referred to as the National ISDN number; the maximum length is 12, 13, or 14 digits, based on the country code.
ISDN subaddress	Identifies one of many devices at the termination point. An ISDN subaddress is similar to an extension on a PBX.

Examples

In the following SVC example, if IP or AppleTalk triggers the call, the SVC is set up with the QoS parameters defined within the class “example”.

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 test source-addr e164 123456 dest-addr e164 654321 clps 2 cdps 4
 ip 10.1.1.1 class example
 appletalk 1000.2 class example
```

Related Commands

Command	Description
class (**map-list**)	Associates a map class with a protocol-and-address combination.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

match fr-de

To match packets on the basis of the Frame Relay discard eligibility (DE) bit setting, use the **match fr-de** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match fr-de

no match fr-de

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched on the basis of the Frame Relay DE bit setting.

Command Modes

Class-map configuration (config-cmap)

Command History

Release	Modification
12.0(25)S	This command was introduced for the Cisco 7500 series router.
12.0(26)S	This command was implemented on the Cisco 7200 series router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was implemented on the Cisco 7300 series router.

Examples

The following example creates a class called match-fr-de and matches packets on the basis of the Frame Relay DE bit setting.

```
Router(config)# class-map match-fr-de
Router(config-cmap)# match fr-de
Router(config-cmap)# end
```

Related Commands

Command	Description
set fr-de	Changes the DE bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.

match protocol (L2TPv3)

To configure protocol demultiplexing, use the **match protocol** command in xconnect configuration mode. To disable protocol demultiplexing, use the **no** form of this command.

match protocol ipv6

no match protocol ipv6

Syntax Description

ipv6	Specifies IPv6 as the protocol to demultiplex.

Command Default

IPv6 protocol demultiplexing is disabled by default.

Command Modes

Xconnect configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

Protocol demultiplexing is supported only for Ethernet and terminated data-link connection identifier (DLCI) Frame Relay traffic in Cisco IOS Release 12.0(29)S and later releases.

Protocol demultiplexing requires supporting the combination of an IP address and an **xconnect** command configuration on the IPv4 provider edge (PE) interface. This combination of configurations is not allowed without enabling protocol demultiplexing, with the exception of switched Frame Relay permanent virtual circuits (PVCs). If no IP address is configured, the protocol demultiplexing configuration is rejected. If an IP address is configured, the **xconnect** command configuration is rejected unless protocol demultiplexing is enabled in xconnect configuration mode before exiting that mode. If an IP address is configured with an **xconnect** command configuration and protocol demultiplexing enabled, the IP address cannot be removed. To change or remove the configured IP address, the **xconnect** command configuration must first be disabled.

Table 20 shows the valid combinations of configurations.

Table 20 Support for the ATM Cell Relay Features

Scenario	IP Address	xconnect Configuration	Protocol Demultiplexing Configuration
Routing	Yes	No	—
L2VPN	No	Yes	No
IPv6 Protocol Demultiplexing	Yes	Yes	Yes

Examples

The following example configures IPv6 protocol demultiplexing in an xconnect configuration:

```
xconnect 10.0.3.201 888 pw-class demux
 match protocol ipv6
```

Related Commands

Command	Description
xconnect	Binds an attachment circuit to a Layer 2 pseudowire and enters xconnect configuration mode

match tcp

To match WAAS Express TCP traffic based on the IP address or port options, use the **match tcp** command in QoS class-map configuration mode. To remove the match, use the **no** form of this command.

match tcp {**any** | **destination** | **source**} {**ip** *ip-address* [*inverse mask*] | **port** *start-port-number* [*end-port-number*]}

match tcp {**any** | **destination** | **source**} {**ip** *ip-address* [*inverse mask*] | **port** *start-port-number* [*end-port-number*]}

Syntax Description

any	Matches based on any of TCP traffic.
destination	Matches the traffic based on the destination IP address or port number.
source	Matches the TCP traffic based on the source IP address or port number.
ip *ip-address* [*inverse mask*]	(Optional) Matches the TCP traffic based on the source or destination IP address and inverse mask.
port	Matches the TCP traffic based on the port number.
start-port-number	The starting port number.
end-port-number	(Optional) The ending port number.

Command Default

Traffic is matched on all TCP traffic.

Command Modes

QoS class-map configuration (config-cmap)

Command History

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

Usage Guidelines

Use this command to match the TCP traffic based on the IP address or port number of the source or destination. If Network Address Translation (NAT) is used, the IP address refers to the inside local address and outside global address.

Note The class-map type of WAAS combines filters using the match-any logical operator. The match-all logical operator is not supported by the WAAS class map. This means that if one match criterion (filters) matches, the entire class map also matches.

Examples

The following example matches traffic having a destination TCP port number from 7000 to 7009:

```
Router(config)# class-map type waas waas_global
Router(config-cmap)# match tcp destination port 7000 7009
```

The following example matches traffic if the following conditions are matched:

- Destination IP address is in the range 209.165.200.225 and destination TCP port is 80.
- Destination IP address is in the range 209.165.200.225 and destination TCP port is 8080.

```
Router(config)# class-map type waas waas_global
Router(config-cmap)# match tcp destination ip 209.165.200.225 0.0.0.31 port 80 80
Router(config-cmap)# match tcp destination ip 209.165.200.225 0.0.0.31 port 8080 8080
```

Related Commands

Command	Description
class-map type waas	Defines a WAAS Express class map.

mls l2tpv3 reserve

To reserve a loopback interface to use as a source for the Layer 2 Tunnel Protocol version 3 (L2TPv3) tunnel for a specific line card and processor pair, use the **mls l2tpv3 reserve** command in interface configuration mode. To cancel the loopback interface reservation, use the **no** form of this command.

mls l2tpv3 reserve {**slot** *slot-num* | **interface** {**TenGigabitEthernet** *slot_num*/*slot_unit* | **GigabitEthernet** *slot_num*/*slot_unit* **GigabitEthernet** *slot_num*/*slot_unit*}}

no mls l2tpv3 reserve {**slot** *slot-num* | **interface** {**TenGigabitEthernet** *slot_num*/*slot_unit* | **GigabitEthernet** *slot_num*/*slot_unit* **GigabitEthernet** *slot_num*/*slot_unit*}}

Syntax Description

slot *slot_num*	Router slot number for a Cisco 7600 series SPA Interface Processor-400 (SIP-400) line card.
interface	Specifies that the interface is for a Cisco 7600 series ES Plus line card.
TenGigabitEthernet	Specifies a 2-Port 10 Gigabit Ethernet or a 4-Port 10 Gigabit Ethernet line card.
GigabitEthernet	Specifies 20-Port Gigabit Ethernet or 40-Port Gigabit Ethernet line cards.
slot_num/*slot_unit*	Slot number in which the line card is inserted and the slot unit (the line card port number). When using two Gigabit Ethernet interfaces, the slot numbers of the two interfaces must match and can either be 1, 11, 21, or 31. The slot unit of the second Gigabit Ethernet interface must be ten plus the slot number of the first Gigabit Ethernet interface.

Command Default

No loopback interface is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.
12.2(33)SRD	This command was modified to support the Cisco 7600 series ES Plus line cards.

Usage Guidelines

This command also prevents the reserved loopback interface from being used across multiple line cards.

Examples

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for a SIP-400 line card:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback1
Router(config-if)# mls l2tpv3 reserve slot 4
Router(config-if)# end
```

```
Router#
*Sep 11 04:03:26.770: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback1
Building configuration...
Current configuration : 69 bytes
!
interface Loopback1
 no ip address
 mls l2tpv3 reserve slot 4
end
```

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for two 40-Port Gigabit Ethernet line cards:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback1
Router(config-if)# mls l2tpv3 reserve interface GigabitEthernet 3/11 GigabitEthernet 3/20
Router(config-if)# end
Router#
*Sep 10 10:46:01.671: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback1
Building configuration...
Current configuration : 112 bytes
!
interface Loopback1
 no ip address
 mls l2tpv3 reserve interface GigabitEthernet3/11 GigabitEthernet3/20
end
```

The following example reserves a loopback interface to use as a source for the L2TPv3 tunnel for a 2-Port 10 Gigabit Ethernet line card:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Loopback2
Router(config-if)# mls l2tpv3 reserve interface TenGigabitEthernet 9/1
Router(config-if)# end
Router#
*Sep 10 10:49:31.451: %SYS-5-CONFIG_I: Configured from console by console
Router# show running interface Loopback2
Building configuration...
Current configuration : 112 bytes
!
interface Loopback2
 no ip address
 mls l2tpv3 reserve interface Tengigether 9/1
end
```

Related Commands

Command	Description
show running interface	Verifies the configuration.

monitor l2tun counters tunnel l2tp

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

monitor l2tun counters tunnel l2tp id *local-id* {**start** | **stop**}

Syntax Description

id *local-id*	Specifies the local ID of an L2TP tunnel.
start	Specifies that per-tunnel control message statistics will be collected for the tunnel.
stop	Specifies that per-tunnel control message statistics will not be collected for the tunnel. **Note** Any existing per-tunnel statistics will be lost when the **stop** keyword is issued.

Command Default

Per-tunnel statistics are not collected for any tunnels.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **monitor l2tun counters tunnel l2tp** command to enable or disable the collection of per-tunnel control message statistics. Per-tunnel statistics must be enabled for each tunnel that you want to monitor.

Use the **show l2tun counters tunnel l2tp id** *local-id* command to display per-tunnel statistics for a specific tunnel. Use the **show l2tun counters tunnel l2tp all** command to display per-tunnel statistics for all tunnels that have per-tunnel statistics enabled.

Use the **clear l2tun counters tunnel l2tp id** *local-id* command to clear the per-tunnel statistics for a specific tunnel. Per-tunnel statistics are also cleared when the collection of per-tunnel statistics is disabled.

Examples

The following example enables the collection of per-tunnel control message statistics for the tunnel with the local tunnel ID 4230:

```
monitor l2tun counters tunnel l2tp id 4230 start
```

The following example disables the collection of per-tunnel control message statistics for the tunnel with the local tunnel ID 4230:

```
monitor l2tun counters tunnel l2tp id 4230 stop
```

Related Commands

Command	Description
clear l2tun counters tunnel l2tp	Clears global or per-tunnel control message statistics for L2TP tunnels.
show l2tun counters tunnel l2tp	Displays global or per-tunnel control message statistics for L2TP tunnels.

neighbor (L2VPN Pseudowire Switching)

To specify the routers that should form a point-to-point Layer 2 virtual forwarding interface (VFI) connection, use the **neighbor** command in L2 VFI point-to-point configuration mode. To disconnect the routers, use the **no** form of this command.

neighbor *ip-address vc-id* {**encapsulation mpls** |**pw-class** *pw-class-name*}

no neighbor *ip-address vc-id* {**encapsulation mpls** |**pw-class** *pw-class-name*}

Syntax Description

ip-address	IP address of the VFI neighbor.
vc-id	Virtual circuit (VC) identifier.
encapsulation mpls	Encapsulation type.
pw-class	Pseudowire type.
pw-class-name	Name of the pseudowire you created when you established the pseudowire class.

Command Default

Routers do not form a point-to-point Layer 2 VFI connection.

Command Modes

L2 VFI point-to-point configuration (config-vfi)

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.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

A maximum of two **neighbor** commands are allowed when you issue an **l2 vfi point-to-point** command.

Examples

The following example is a typical configuration of a Layer 2 VFI connection:

```
Router(config)# l2 vfi atom point-to-point
Router(config-vfi)# neighbor 10.10.10.10 1 encapsulation mpls
```

Related Commands

Command	Description
l2 vfi point-to-point	Establishes a point-to-point Layer 2 VFI between two separate networks.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]

no neighbor *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Defaults

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Router(config-vfi)# l2 vfi vfi-1 manual
Router(config-vfi)# vpn 1
Router(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Router(config-vfi)# l2 vfi vfi-1 manual
Router(config-vfi)# vpn 1
Router(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

oam-ac emulation-enable

To enable Operation, Administration, and Maintenance (OAM) cell emulation on ATM adaptation layer 5 (AAL5) over Multiprotocol Label Switching (MPLS) or Layer 2 Tunnel Protocol Version 3 (L2TPv3), use the **oam-ac emulation-enable command in the appropriate** configuration mode on both provider edge (PE) routers**.** To disable OAM cell emulation, use the **no** form of this command on both routers.

oam-ac emulation-enable [*seconds*]

no oam-ac emulation-enable [*seconds*]

Syntax Description

seconds	(Optional) The rate (in seconds) at which the alarm indication signal (AIS) cells should be sent. The range is 0 to 60 seconds. If you specify 0, no AIS cells are sent. The default is 1 second, which means that one AIS cell is sent every second.

Command Default

OAM cell emulation is disabled.

Command Modes

L2transport VC configuration—for an ATM PVC
VC class configuration mode—for a VC class

Command History

Release	Modification
12.0(23)S	This command was introduced.
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.
12.0(30)S	This command was updated to enable OAM cell emulation 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(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is used with AAL5 over MPLS or L2TPv3 and is not supported with ATM cell relay over MPLS or L2TPv3.

Examples

The following example shows how to enable OAM cell emulation on an ATM permanent virtual circuit (PVC):

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable
```

The following example shows how to set the rate at which an AIS cell is sent every 30 seconds:

```
Router# interface ATM 1/0/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm oamclass
Router(config-vc-class)# encapsulation aal5
Router(config-vc-class)# oam-ac emulation-enable 30
Router(config-vc-class)# oam-pvc manage
Router(config)# interface atm1/0
Router(config-if)# class-int oamclass
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.

optimize

To apply WAAS Express optimization, use the **optimize** command in QoS policy-map configuration mode. To remove the optimization, use the **no** form of this command.

optimize tfo{**dre** | **lz**} **application** *application-name*

no optimize tfo{**dre** | **lz**} **application** *application-name*

Syntax Description

tfo	Applies Transport Flow Optimization (TFO) only.
dre	Applies Data Redundancy Elimination (DRE) and TFO.
lz	Applied Lempel-Ziv (LZ) and TFO.
application *application-name*	Class-map application name.

Command Default

The default optimization is pass-through.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

Use this command to apply optimizations for WAN traffic.

Cisco WAAS Express uses a variety of TFO features to optimize TCP traffic intercepted by the WAAS devices. TFO protects communicating clients and servers from negative WAN conditions, such as bandwidth constraints, packet loss, congestion, and retransmission. Cisco WAAS Express uses the following optimization technologies based on the type of traffic it encounters:

- TFO—A collection of optimization technologies such as automatic windows scaling, increased buffering, and selective acknowledgment that optimize all TCP traffic over your network.
- DRE—A compression technology that reduces the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. DRE operates on significantly larger streams and maintains a much larger compression history than LZ compression.
- LZ—A compression technology that operates on smaller data streams and keeps limited compression history compared to RE.

Note If you do not use this command, pass-through optimization is applied on the WAN traffic.

Examples

This example creates a new policy with WAAS Express actions and application tagging:

```
Router(config)# policy-map type waas_global
```

```
Router(config-pmap)# class AFS
Router(config-pmap-c)# optimize tfo lz application Filesystem
Router(config-pmap-c)# exit
Router(config-pmap)# class Http
Router(config-pmap-c)# optimize tfo dre lz application Web
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
passthrough	Allows traffic without optimization.
policy-map type waas	Defines a WAAS Express policy map.
sequence-interval	Assigns sequential numbering to the class maps.

packet drop during-authorization

To specify that packets received from the user during authorization will be dropped, use the **packet drop during-authorization** command in transparent auto-logon configuration mode. To remove the configuration, use the **no** form of this command.

packet drop during-authorization

no packet drop during-authorization

Syntax Description

This command has no arguments or keywords.

Defaults

Packet drop during authorization is disabled, and packets from the authorizing user are forwarded.

Command Modes

Transparent auto-logon configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(3)B	This command was integrated into Cisco IOS Release 12.3(3)B.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Use this command for configuring data traffic packet drop for users that are waiting for authorization (WA).

Examples

The following example specifies that packets received from the user during authorization will be dropped:

```
Router(config-login-transparent)# packet drop during-authorization
```

Related Commands

Command	Description
ssg login transparent	Enables the SSG Transparent Autologon feature.

parameter-map type waas

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

parameter-map type waas *parameter-map-name*

no parameter-map type waas *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map. **Note** The only parameter-map type supported is **waas_global**.

Command Default

Global parameters 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 **parameter-map type** command and enters parameter-map configuration mode. The parameter map type of WAAS can be deleted only if WAAS Express is not enabled on any interface.

Examples

The following example shows how to configure global parameters for WAAS Express:

```
Router> enable
Router# configure terminal
Router(config)# parameter-map type waas waas_global
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
cpu-threshold	Sets the CPU threshold limit.
lz entropy-check	Enables entropy checking to turn on LZ compression.
parameter-map type	Creates or modifies a parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery blacklist	Configures a blacklist with autodiscovery for WAAS Express.
tfo optimize	Configures compression for WAAS Express.
waas config	Restores or removes WAAS Express default configurations.

passthrough

To pass through match traffic and not apply the WAN optimization, use the **passthrough** command in QoS policy-map class configuration mode. To remove the default optimization, use the **no** form of this command.

passthrough application *application-name*

no passthrough application *application-name*

Syntax Description

application *application-name*	Specifies the class-map application name.

Command Default

The default optimization is pass-through.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

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

Usage Guidelines

Use this command if you do not want to specify any optimizations such as Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (LZ) for WAN traffic.

Examples

The following example shows how to specify pass-through optimization for Instant-Messaging:

```
Router(config)# policy-map type waas waas_global
Router(config-pmap)# sequence-interval 111
Router(config-pmap-c)# optimize tfo dre lz application File-System
Router(config-pmap-c)# passthrough application Instant-Messaging
Router(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
policy-map type waas	Defines a WAAS Express policy map.
optimize	Applies WAAS optimization.
sequence-interval	Assigns sequential numbering to class maps.

password

To configure the password used by a provider edge (PE) router for Challenge Handshake Authentication Protocol (CHAP) style Layer 2 Tunnel Protocol Version 3 (L2TPv3) authentication, use the **password** command in L2TP class configuration mode. To disable a configured password, use the **no** form of this command.

password [**0** | **7**] *password*

no password

Syntax Description

[0 | 7]	(Optional) Specifies the input format of the shared secret. • **0**—Specifies that a plain-text secret will be entered. • **7**—Specifies that an encrypted secret will be entered. The default value is **0**.
password	The password used for L2TPv3 authentication.

Defaults

If a password is not configured for the L2TP class with the **password** command, the password configured with the **username password** command in global configuration mode is used. The default input format of the shared secret is **0**.

Command Modes

L2TP class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The password hierarchy sequence used for a local and remote peer PE for L2TPv3 authentication is as follows:

- The L2TPv3 password (configured with the **password** command) is used first.
- If no L2TPv3 password exists, the globally configured password (configured with the **username password** command) for the router is used.

Note The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **password**, results in incorrect translation.

Examples

The following example sets the password named tunnel2 to be used to authenticate an L2TPv3 session between the local and remote peers in L2TPv3 pseudowires configured with the L2TP class configuration named l2tp class1:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# authentication
Router(config-l2tp-class)# password tunnel2
```

Related Commands

Command	Description
authentication	Enables L2TPv3 CHAP-style authentication.
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 (L2TP)

To configure the password used by a provider edge (PE) router for Layer 2 authentication, use the **password** command in L2TP class configuration mode. To disable a configured password, use the **no** form of this command.

password [*encryption-type*] *password*

no password [*encryption-type*] *password*

Syntax Description

encryption-type	(Optional) Specifies the type of encryption to use. The valid values are from 0 to 7. Currently defined encryption types are 0 (no encryption) and 7 (text is encrypted using an algorithm defined by Cisco). The default encryption type is 0.
password	Specifies the password used for L2TPv3 authentication.

Command Default

If a password is not configured for the L2TP class with the **password** command, the password configured with the **username** command in global configuration mode is used.

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(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 password that you define with the **password** command is also used for attribute-value pair (AVP) hiding.

The password hierarchy sequence used for a local and remote peer PE for L2TPv3 authentication is as follows:

- The L2TPv3 password (configured with the **password** command) is used first.
- If no L2TPv3 password exists, the globally configured password (configured with the **username password** command) for the router is used.

Examples

The following example sets the password named “tunnel2” to be used to authenticate an L2TPv3 session between the local and remote peers in L2TPv3 pseudowires that has been configured with the L2TP class configuration named “l2tp-class1”:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# authentication
Router(config-l2tp-class)# password tunnel2
```

Related Commands

Command	Description
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.
username	Establishes a username-based authentication system.

policy-map type mace

To configure a Measurement, Aggregation, and Correlation Engine (MACE) policy map and enter policy map configuration mode, use the **policy-map type mace** command in global configuration mode. To remove a MACE policy map, use the **no** form of this command.

policy-map type mace *name*

no policy-map type mace *name*

Syntax Description

name	Name of the MACE policy map. The only accepted value for this argument is **mace_global**.

Command Default

No MACE policy map is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use the **policy-map type mace** command to classify session traffic and run MACE on that traffic. Two types of class maps are supported in a MACE policy map:

- A quality of service (QoS) class map (default type class map)
- A Wide Area Application Services (WAAS) class map

The usage of QoS and WAAS class maps in the MACE policy is independent of QoS or WAAS policies being configured on the routers.

Inside a MACE policy map, you can configure a flow monitor name using only the **flow monitor** command. The name of the flow monitor is used to collect the corresponding flow metrics and to export these flow metrics when the cache timeout is updated.

Note Only one flow monitor can be configured in a class map.

Examples

The following example shows how to configure the MACE policy map, mace_global:

```
Router(config)# policy-map type mace mace_global
Router(config-pmap)# class class1
Router(config-pmap-c)# flow monitor name my-flow-monitor
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy.
flow monitor	Creates or modifies a Flexible NetFlow flow monitor.
policy-map	Enters policy-map configuration mode, and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.

policy-map type waas

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

policy-map type waas *policy-map-name*

no policy-map type waas *policy-map-name*

Syntax Description

policy-map-name	Name of the class map. **Note** The only policy-map type supported is **waas_global**.

Command Default

No WAAS Express policy maps are configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command extends the **policy-map** command and enters QoS policy-map configuration mode. The policy-map type of WAAS can be deleted only if WAAS Express is not enabled on any interface.

Examples

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

```
Router> enable
Router# configure terminal
Router(config)# policy-map type waas waas_global
Router(config-pmap)# class waas_global
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
optimize	Applies optimization to WAN network traffic.
parameter-map type waas	Configures WAAS Express global parameters.
passthrough	Sends the network traffic without applying any optimization.
policy-map	Creates or modifies a policy map.
sequence-interval	Assigns sequential numbering to class maps.
waas config	Restores or removes WAAS Express default configurations.

precedence (Frame Relay VC-bundle-member)

To configure the precedence levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **precedence** command in Frame Relay VC-bundle-member configuration mode. To remove the precedence level configuration from a PVC, use the **no** form of this command.

precedence {*level* | **other**}

no precedence

Syntax Description

level	The precedence level or levels for the Frame Relay PVC bundle member. The range is from 0 to 7: • 0—routine • 1—priority • 2—immediate • 3—flash • 4—flash override • 5—critical • 6—internetwork control • 7—network control A PVC bundle member can be configured with a single precedence level, multiple individual precedence levels, a range of precedence levels, multiple ranges of precedence levels, or a combination of individual precedence levels and ranges. Examples are as follows: • 0 • 0,2,3 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining precedence levels that are not explicitly configured on any other bundle member PVCs.

Defaults

Precedence levels are not configured.

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

Assignment of precedence levels to PVC bundle members lets you create differentiated services, because you can distribute the IP precedence levels over the various PVC bundle members. You can map a single precedence level or a range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different precedence levels.

Use the **precedence other** command to indicate that a PVC can carry traffic marked with precedence levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **precedence other** command.

This command is available only when the match type for the PVC bundle is set to precedence by using the **match precedence** command in Frame Relay VC-bundle configuration mode.

You can overwrite the precedence level configuration on a PVC by reentering the **precedence** command with a new level value.

All precedence levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member without a precedence level associated with it. As long as all valid precedence levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no precedence level configured will not participate in it.

A precedence level can be configured on one PVC bundle member per bundle. If you configure the same precedence level on more than one PVC within a bundle, the following error appears on the console:

```
%Overlapping precedence levels
```

When you use the **mpls ip** command to enable multiprotocol label switching (MPLS) on the interface, MPLS and IP packets can flow across the interface, and PVC bundles that are configured for IP precedence mapping are converted to MPLS EXP mapping. The PVC bundle functionality remains the same with respect to priority levels, bumping, and so on, but the **match precedence** command is replaced by the **match exp** command, and each **precedence** command is replaced by the **exp** command. The result is that a bundle-member PVC previously configured to carry precedence level 1 IP traffic now carries EXP level 1 MPLS traffic.

When MPLS is disabled, the **match precedence** and **match dscp** commands are restored, and the **exp** commands are replaced by **precedence** commands.

When MPLS is enabled or disabled, PVC bundles configured for IP precedence mapping or MPLS EXP mapping will stay up, and traffic will be transmitted over the appropriate bundle-member PVCs.

Examples

The following example shows how to configure Frame Relay PVC bundle member 101 to carry traffic with IP precedence level 5:

```
frame-relay vc-bundle bundle1
 match precedence
 pvc 101
 precedence 5
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
match dscp	Configures a specific IP differentiated service code point (DSCP) value as a match criterion.
match precedence	Configures IP precedence values as match criteria.
protect (Frame Relay VC-bundle-member)	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

protect (Frame Relay VC-bundle-member)

To configure a Frame Relay permanent virtual circuit (PVC) bundle member with protected group or protected PVC status, use the **protect** command in Frame Relay VC-bundle-member configuration mode. To remove the protected status from a PVC, use the **no** form of this command.

protect {**group** | **vc**}

no protect {**group** | **vc**}

Syntax Description

group	Configures the PVC bundle member as part of a collection of protected PVCs within the PVC bundle.
vc	Configures the PVC member as individually protected.

Command Default

The PVC is not in a protected group and is also not individually protected.

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

When an individually-protected PVC goes down, it takes the bundle down. When all members of a protected group go down, the bundle goes down.

Despite any protection configurations, the PVC bundle will go down if a downed PVC has no PVC to which to bump its traffic or if the last PVC that is up in a PVC bundle goes down.

Examples

The following example configures Frame Relay PVC bundle member 101 as an individually protected PVC:

```
frame-relay vc-bundle new york
 pvc 101
  protect vc
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a 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.

protocol (L2TP)

To specify the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session and to cause control plane configuration settings to be taken from a specified L2TP class, use the **protocol** command in pseudowire class configuration mode. To remove the signaling protocol (and the control plane configuration to be used) from a pseudowire class, use the **no** form of this command.

protocol {**l2tpv2** | **l2tpv3** | **none**} [*l2tp-class-name*]

no protocol {**l2tpv2** | **l2tpv3** | **none**} [*l2tp-class-name*]

Syntax Description

l2tpv2	Specifies that the Layer 2 Tunnel Protocol (L2TP) signaling protocol will be used.
l2tpv3	Specifies that the L2TPv3 signaling protocol will be used. This is the default.
none	Specifies that no signaling protocol will be used in L2TPv3 sessions.
l2tp-class-name	(Optional) The name of the L2TP class whose control plane configuration is to be used for pseudowires set up from a specified pseudowire class. If you do not enter a value for the *l2tp-class-name* argument, the default control plane configuration settings in the L2TP signaling protocol are used.

Command Default

The default protocol is **l2tpv3**.

Command Modes

Pseudowire 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

Use the **protocol** (L2TP) command to configure the signaling protocol to use in sessions created from the specified pseudowire class. In addition, you can use this command to specify the L2TP class (see the "Configuring the Xconnect Attachment Circuit" section in the *Layer 2 Tunnel Protocol Version 3* feature document) from which the control plane configuration settings are to be taken.

Use the **protocol none** command to specify that no signaling will be used in L2TPv3 sessions created from the specified pseudowire class. This configuration is required for interoperability with a remote peer running the Universal Tunnel Interface (UTI).

Do not use this command if you want to configure a pseudowire class that will be used to create manual L2TPv3 sessions (see the "Static L2TPv3 Sessions" section in the *Layer 2 Tunnel Protocol Version 3* feature document).

Examples

The following example shows how to enter pseudowire class configuration mode and how to configure L2TPv3 as the signaling protocol. The control plane configuration used in the L2TP class named "class1" will be used to create dynamic L2TPv3 sessions for a VLAN xconnect interface.

```
Router(config)# pseudowire-class vlan-xconnect
Router(config-pw)# protocol l2tpv3 class1
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

pseudowire

To bind an attachment circuit to a Layer 2 pseudowire for xconnect service, use the **pseudowire** command in interface configuration mode.

pseudowire *peer-ip-address vcid* **pw-class** *pw-class-name* [**sequencing** {**transmit** | **receive** | **both**}]

Syntax Description

peer-ip-address	The IP address of the remote peer.
vcid	The 32-bit identifier of the virtual circuit between the routers at each end of the Layer 2 control channel.
pw-class *pw-class-name*	The pseudowire class configuration from which the data encapsulation type will be taken.
sequencing {**transmit** | **receive** | **both**}	(Optional) Sets the sequencing method to be used for packets received or sent in L2TP sessions: • **transmit**—Sequencing of Layer 2 Tunnel Protocol (L2TP) data packets received from the session. • **receive**—Sequencing of L2TP data packets sent into the session. • **both**—Sequencing of L2TP data packets that are both sent and received from the session.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each pseudowire configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

The same *vcid* value that identifies the attachment circuit must be configured using the **pseudowire** command on the local and remote router at each end of a Layer 2 session. The virtual circuit identifier creates the binding between a pseudowire and an attachment circuit.

The **pw-class** *pw-class-name* value binds the pseudowire configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **pseudowire** command.

Examples

The following example creates a virtual-PPP interface with the number 1, configures PPP on the virtual-PPP interface, and binds the attachment circuit to a Layer 2 pseudowire for xconnect service for the pseudowire class named pwclass1:

```
interface virtual-ppp 1
 ppp authentication chap
 ppp chap hostname peer1
 pseudowire 172.24.13.196 10 pw-class pwclass1
```

Related Commands

Command	Description
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.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

pseudowire-class

To specify the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class [*pw-class-name*]

no pseudowire-class [*pw-class-name*]

Syntax Description

pw-class-name	(Optional) The name of a Layer 2 pseudowire class. If you want to configure more than one pseudowire class, you must enter a value for the *pw-class-name* argument.

Command Default

No pseudowire classes are defined.

Command Modes

Global 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

The **pseudowire-class** command allows you to configure a pseudowire class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

After you enter the **pseudowire-class** command, the router switches to pseudowire class configuration mode, where pseudowire settings may be configured.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)#
```

Related Commands

Command	Description
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.
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

pvc (Frame Relay VC-bundle)

To create a permanent virtual circuit (PVC) that is a Frame Relay PVC bundle member, and to enter Frame Relay VC-bundle-member configuration mode, use the **pvc** command in Frame Relay VC-bundle configuration mode. To delete a PVC from the Frame Relay PVC bundle, use the **no** form of this command.

pvc *dlci* [*vc-name*]

no pvc *dlci* [*vc-name*]

Syntax Description

dlci	Data-link connection identifier (DLCI) number used to identify the PVC.
vc-name	(Optional) Alphanumeric name for the PVC.

Command Default

No PVC is defined.

Command Modes

Frame Relay VC-bundle 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

To use this command, you must first create a Frame Relay PVC bundle and enter Frame Relay VC-bundle configuration mode.

A PVC bundle must have at least one PVC for the bundle to come up. A PVC bundle cannot have more than eight PVCs. If you try to configure more than eight PVCs in a bundle, the following message appears on the console:

```
%FR vc-bundle contains 8 members. Cannot add another.
```

Dynamic PVCs can be specified as PVC bundle members; however, if a PVC has already been created by using another configuration command, you cannot add it to a PVC bundle. If you try to do so, the following message appears on the console:

```
%DLCI 200 is not a dynamic PVC. Cannot add to VC-Bundle.
```

If a PVC is already a member of a PVC bundle, any attempt to reuse that same PVC in a command that creates a PVC (for example, **frame-relay interface-dlci** or **frame-relay local-dlci**) causes the following error message:

```
%Command is inapplicable to vc-bundle PVCs.
```

Examples

The following example creates a PVC that has a DLCI number of 101 and that belongs to a Frame Relay PVC bundle named new_york:

```
frame-relay vc-bundle new_york
 pvc 101
```

Related Commands

Command	Description
dscp (frame-relay vc-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
exp	Configures MPLS EXP levels for a Frame Relay PVC bundle member.
frame-relay vc-bundle	Creates a Frame Relay PVC bundle and enters Frame Relay VC-bundle configuration mode.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

rd (VPLS)

To specify the route distinguisher (RD) to distribute endpoint information in a Virtual Private LAN Service (VPLS) configuration, use the **rd** command in L2 VFI configuration mode. To remove the manually configured RD and return to the automatically generated RD, use the **no** form of this command.

rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

no rd {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:nn	Specifies a 16-bit autonomous system number and 32-bit arbitrary number. The autonomous system number does not have to match the local autonomous system number.
ip-address:nn	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

VPLS Autodiscovery automatically generates a route distinguisher using the Border Gateway Protocol (BGP) autonomous system number and the configured virtual forwarding instance (VFI) Virtual Private Network (VPN) ID.

Command Modes

L2 VFI configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

VPLS Autodiscovery automatically generates a route distinguisher using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated route distinguisher.

The same RD value cannot be configured in multiple VFIs.

There are two formats for configuring the route distinguisher argument. It can be configured in the *autonomous-system-number*:*network-number* format, or it can be configured in the *IP address*:*network-number* format.

An RD is either:

- autonomous system-related—Composed of an autonomous system number and an arbitrary number.
- IP address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit-autonomous-system-number:*32-bit-number*
For example, 101:3.

32-bit-IP-address:*16-bit-number*
For example, 192.168.122.15:1.

Examples

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an IP address of 10.4.4.4 and a network address of 70:

```
l2 vfi SP2 autodiscovery
 vpn id 200
 vpls-id 10.4.4.4:70
 rd 10.4.5.5:7
```

The following example shows a configuration using VPLS Autodiscovery that sets the RD to an autonomous system number of 2 and a network address of 3:

```
l2 vfi SP2 autodiscovery
 vpn id 200
 vpls-id 10.4.4.4:70
 rd 2:3
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enable a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

receive-window

To configure the packet size of the receive window on the remote provider edge router at the other end of a Layer 2 control channel, use the **receive-window** command in L2TP class configuration mode. To disable the configured value, use the **no** form of this command.

receive-window *number*

no receive-window *number*

Syntax Description

number	The number of packets that can be received by the remote peer before backoff queueing occurs. The valid values range from 1 to the upper limit the peer has for receiving packets. The default value is the upper limit that the remote peer has for receiving packets.

Command Default

The default packet size of the receive window is the upper limit that the remote peer has for receiving packets.

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

To determine the upper limit for the *number* argument, refer to the platform-specific documentation for the peer router.

Examples

The following example sets a receive window of 30 packets to the remote peer in Layer 2 pseudowires that have been configured with the L2TP class named" l2tp-class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# receive-window 30
```

Related Commands

Command	Description
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.

retransmit

To configure the retransmission settings of control packets, use the **retransmit** command in L2TP class configuration mode. To disable the configured values, use the **no** form of this command.

retransmit {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *seconds*}

no retransmit {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *seconds*}

Syntax Description

initial retries *initial-retries*	Specifies how many start control channel requests (SCCRQs) are re-sent before giving up on the session. Valid values for the *initial-retries* argument range from 1 to 1000. The default value is 2
retries *retries*	Specifies how many retransmission cycles occur before determining that the peer provider edge (PE) router does not respond. Valid values for the *retries* argument range from 1 to 1000. The default value is 15.
timeout {**max** | **min**} *seconds*	Specifies maximum and minimum retransmission intervals (in seconds) for resending control packets. Valid values for the *timeout* argument range from 1 to 8. The default maximum interval is 8; the default minimum interval is 1.

Command Default

The default values of the retransmission settings are used.

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

Use this command to configure the amount of time spent trying to establish or maintain a control channel.

Examples

The following example configures ten retries for sending tunneled packets to a remote peer in Layer 2 pseudowires that have been configured with the Layer 2 Tunnel Protocol (L2TP) class named "l2tp-class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# retransmit retries 10
```

Related Commands

Command	Description
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.

rewrite ingress tag

To specify the encapsulation adjustment to be performed on a frame ingressing a service instance, use the **rewrite ingress tag** command in service instance configuration mode. To delete the encapsulation adjustment, use the **no** form of this command.

rewrite ingress tag {**pop** {**1** | **2**} [**symmetric**] | **push** {**dot1ad** *vlan-id* [**dot1q** *vlan-id*] [**symmetric**] | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] [**symmetric**]} | **translate** {**1-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**symmetric**] | **1-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id*} [**symmetric**] | {**2-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id*} [**symmetric**] | **2-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* **second-dot1q** *vlan-id*} [**symmetric**]}

no rewrite ingress tag

Syntax on the Cisco ASR 1000 Series Aggregation Router

rewrite ingress tag {**pop** {**1** | **2**} [**symmetric**] | **push** {**dot1ad** *vlan-id* [**dot1q** *vlan-id*] [**symmetric**] | **dot1q** *vlan-id* [**second-dot1q** *vlan-id*] [**symmetric**] | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} [**second-dot1q** *vlan-id*] [**symmetric**]} | **translate** {**1-to-1** {**dot1ad** *vlan-id* | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}] [**symmetric**]} | **1-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* | **dot1q** *vlan-id* {**second-dot1q** *vlan-id* | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*}} [**symmetric**] | **2-to-1** {**dot1ad** *vlan-id* [**symmetric**] | **dot1q** *vlan-id* [**vlan-type** {**0x88a8** | **0x9100** | **0x9200**}] [**symmetric**]} | **2-to-2** {**dot1ad** *vlan-id* **dot1q** *vlan-id* [**symmetric**] | **dot1q** *vlan-id* {**second-dot1q** *vlan-id* | **vlan-type** {**0x88a8** | **0x9100** | **0x9200**} **second-dot1q** *vlan-id*} [**symmetric**]}}

no rewrite ingress tag

Syntax Description

pop	Removes a tag from a packet.
{**1** | **2**}	Specifies either the outermost tag or the two outermost tags for removal from a packet.
symmetric	(Optional) Indicates a reciprocal adjustment to be done in the egress direction. For example, if the ingress pops a tag, the egress pushes a tag and if the ingress pushes a tag, the egress pops a tag.
push	Adds a tag.
dot1ad	Specifies an IEEE 802.1ad tag.
vlan-id	Integer in the range 1 to 4094 that identifies the VLAN.
dot1q	Specifies an IEEE 802.1Q tag.
second-dot1q	Specifies a different 802.1Q tag at the ingress service instance.
vlan-type	Specifies the type of VLAN protocol.
0x88a8	Specifies the protocol type 0x88a8.
0x9100	Specifies the protocol type 0x9100.
0x9200	Specifies the protocol type 0x9200.
translate	Translates, by VLAN ID, a tag or a pair of tags defined in the **encapsulation** command.

1-to-1	Translates a single tag defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
1-to-2	Translates a single tag defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.
2-to-1	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a single tag defined in the **rewrite ingress tag** command.
2-to-2	Translates, by VLAN ID, a pair of tags defined by the **encapsulation** command to a pair of tags defined in the **rewrite ingress tag** command.

Command Default

The frame is left intact on ingress (the service instance is equivalent to a trunk port).

Command Modes

Service instance configuration (config-if-srv)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

The **symmetric** keyword is accepted for all rewrite operations only when a single VLAN is configured in encapsulation. If a list of VLANs or a range of VLANs is configured in encapsulation, the **symmetric** keyword is accepted only for push rewrite operations.

The **pop** keyword assumes the elements being popped are defined by the encapsulation type. The exception case should be drop the packet.

The **translate** keyword assumes the tags being translated from are defined by the encapsulation type. In the 2-to-1 option, the “2” means 2 tags of a type defined by the **encapsulation** command. The translation operation requires at least one “from” tag in the original packet. If the original packet contains more tags than the ones defined in the “from,” the operation should be done beginning on the outer tag. Exception cases should be dropped.

Examples

The following example shows how to specify the encapsulation adjustment to be performed on the frame ingressing the service instance:

```
Router> enable
Router# configure terminal
Router(config) interface gigabitethernet 2/0/0
Router(config-if)# service instance 100 ethernet
Router(config-if-srv)# encapsulation dot1q 100
Router(config-if-srv)# rewrite ingress tag push dot1q 200
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by an interface.

route-target (VPLS)

To specify a route target (RT) for a Virtual Private LAN Service (VPLS) virtual forwarding instance (VFI), use the **route-target** command in L2 VFI configuration mode. To revert to the automatically-generated route target, use the **no** form of this command.

route-target [**import** | **export** | **both**] {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

no route-target {**import** | **export** | **both**} {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

import	(Optional) Imports routing information from the target virtual private network (VPN) extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
autonomous-system-number:*nn*	The autonomous system number and a 32-bit number.
ip-address:*nn*	The IP address and a 16-bit number.

Defaults

VPLS Autodiscovery automatically generates a route target using the lower six bytes of the route distinguisher (RD) and VPLS ID.

Command Modes

L2 VFI configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The same route target cannot be configured in multiple VFIs.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

16-bit-autonomous-system-number:*32-bit-number*
For example, 101:3.

32-bit-IP-address:*16-bit-number*
For example, 192.168.122.15:1.

Examples

The following example shows a VPLS Autodiscovery configuration that configures route-target extended community attributes for VFI SP1:

```
l2 vfi SP1 autodiscovery
 vpn id 100
 vpls-id 5:300
 rd 4:4
 route-target 10.1.1.1:29
```

Related Commands

Command	Description
auto-route-target	Automatically generates the route target in a VFI.
l2 vfi autodiscovery	Enable a VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

sequence-interval

To assign sequential numbers to class maps, use the **sequence-interval** command in QoS policy-map configuration mode. To remove the numbers, use the **no** form of this command.

sequence-interval *number*

no sequence-interval *number*

Syntax Description

number	The sequential interval. The range is 1 to 65535.

Command Default

Class maps are not assigned with sequential numbers.

Command Modes

QoS policy-map configuration (config-pmap)

Command History

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

Usage Guidelines

Use this command to assigns sequential numbers to the class maps at a specific interval.

Examples

The following example sets the interval as 100 to assign sequence numbers to class maps:

```
Router(config)# policy-map type waas waas_global
Router(config-pmap)# sequence-interval 100
```

Related Commands

Command	Description
class	Associates a map class with a specified DLCI.
passthrough	Allows traffic without optimization.
policy-map type waas	Defines a WAAS Express policy map.
optimize	Applies WAAS optimization.

sequencing

To configure the direction in which sequencing is enabled for data packets in a Layer 2 pseudowire, use the **sequencing** command in pseudowire class configuration mode. To remove the sequencing configuration from the pseudowire class, use the **no** form of this command.

sequencing {**transmit** | **receive** | **both** | **resync** *number*}

no sequencing {**transmit** | **receive** | **both** | **resync** *number*}

Syntax Description

transmit	Updates the Sequence Number field in the headers of data packets sent over the pseudowire according to the data encapsulation method that is used.
receive	Keeps the value in the Sequence Number field in the headers of data packets received over the pseudowire. Out-of-order packets are dropped.
both	Enables both the **transmit** and **receive** options.
resync	Enables the reset of packet sequencing after the disposition router receives a specified number of out-of-order packets.
number	The number of out-of-order packets that cause a reset of packet sequencing. The range is 5 to 65535.

Command Default

Sequencing is disabled.

Command Modes

Pseudowire class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced for Layer 2 Tunnel Protocol Version 3 (L2TPv3).
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.0(29)S	This command was updated to support Any Transport over MPLS (AToM).
12.0(30)S	The **resync** keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	L2TPv3 support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	AToM support for this command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

When you enable sequencing using any of the available options, the sending of sequence numbers is automatically enabled and the remote provider edge (PE) peer is requested to send sequence numbers. Out-of-order packets received on the pseudowire are dropped only if you use the **sequencing receive** or **sequencing both** command.

If you enable sequencing for Layer 2 pseudowires on the Cisco 7500 series routers and you issue the **ip cef distributed** command, all traffic on the pseudowires is switched through the line cards.

It is useful to specify the **resync** keyword for situations when the disposition router receives many out-of-order packets. It allows the router to recover from situations where too many out-of-order packets are dropped.

Examples

The following example shows how to enable sequencing in data packets in Layer 2 pseudowires that were created from the pseudowire class named "ether-pw" so that the Sequence Number field is updated in tunneled packet headers for data packets that are both sent and received over the pseudowire:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1000 out-of-order packets:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation mpls
Router(config-pw)# sequencing both
Router(config-pw)# sequencing resync 1000
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the Route Processor card.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

service pad

To enable all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers, use the **service pad** command in global configuration mode. To disable this service, use the **no** form of this command.

service pad [**cmns**] [**from-xot**] [**to-xot**]

no service pad [**cmns**] [**from-xot**] [**to-xot**]

Syntax Description

cmns	(Optional) Specifies sending and receiving PAD calls over CMNS.
from-xot	(Optional) Accepts XOT to PAD connections.
to-xot	(Optional) Allows outgoing PAD calls over XOT.

Command Default

All PAD commands and associated connections are enabled. PAD services over XOT or CMNS are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **cmns** keyword was 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The keywords **from-xot** and **to-xot** enable PAD calls to destinations that are not reachable over physical X.25 interfaces, but instead over TCP tunnels. This feature is known as PAD over XOT (X.25 over TCP).

Examples

If the **service pad** command is disabled, the **pad** EXEC command and all PAD related configurations, such as X.29, are unrecognized, as shown in the following example:

```
Router(config)# no service pad
Router(config)# x29 ?
% Unrecognized command
Router(config)# exit
Router# pad ?
% Unrecognized command
```

If the **service pad** command is enabled, the **pad** EXEC command and access to an X.29 configuration are granted as shown in the following example:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service pad
Router(config)# x29 ?
access-list       Define an X.29 access list
inviteclear-time  Wait for response to X.29 Invite Clear message
profile           Create an X.3 profile
Router# pad ?
WORD   X121 address or name of a remote system
```

In the following example, PAD services over CMNS are enabled:

```
! Enable CMNS on a nonserial interface
interface ethernet0
 cmns enable
!
!Enable inbound and outbound PAD over CMNS service
service pad cmns
!
! Specify an X.25 route entry pointing to an interface's CMNS destination MAC address
x25 route ^2193330 interface Ethernet0 mac 00e0.b0e3.0d62

Router# show x25 vc

SVC 1,  State: D1,  Interface: Ethernet0
     Started 00:00:08, last input 00:00:08, output 00:00:08

     Line: 0   con 0    Location: console Host: 2193330
      connected to 2193330 PAD <--> CMNS Ethernet0 00e0.b0e3.0d62

     Window size input: 2, output: 2
     Packet size input: 128, output: 128
     PS: 2  PR: 3  ACK: 3  Remote PR: 2  RCNT: 0  RNR: no
     P/D state timeouts: 0  timer (secs): 0
     data bytes 54/19 packets 2/3 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Related Commands

Command	Description
cmns enable	Enables the CMNS on a nonserial interface.
show x25 vc	Displays information about active SVCs and PVCs.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

service pad from-xot

To permit incoming X.25 over TCP (XOT) calls to be accepted as a packet assembler/disassembler (PAD) session, use the **service pad from-xot** command in global configuration mode. To disable this service, use the **no** form of this command.

service pad from-xot

no service pad from-xot

Syntax Description

This command has no arguments or keywords.

Defaults

Incoming XOT connections are ignored.

Command Modes

Global configuration

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

If the **service pad from-xot** command is enabled, the calls received using the XOT service may be accepted for processing a PAD session.

Examples

The following example prevents incoming XOT calls from being accepted as a PAD session:

```
no service pad from-xot
```

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).
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

service pad to-xot

To permit outgoing PAD sessions to use routes to an XOT destination, use the **service pad to-xot** command in global configuration mode. To disable this service, use the **no** form of this command.

service pad to-xot

no service pad to-xot

Syntax Description

This command has no arguments or keywords.

Defaults

XOT routes pointing to XOT are not considered.

Command Modes

Global configuration

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.

Examples

If the **service pad to-xot** command is enabled, the configured routes to XOT destinations may be used when the router determines where to send a PAD Call, as shown in the following example:

```
service pad to-xot
```

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).
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

service translation

To enable upper layer user protocol encapsulation for Frame Relay-to-ATM Service Interworking (FRF.8) feature, which allows mapping between encapsulated ATM protocol data units (PDUs) and encapsulated Frame Relay PDUs, use the **service translation** command in FRF.8 connect configuration mode. To disable upper layer user protocol encapsulation, use the **no** form of this command.

service translation

no service translation

Syntax Description

This command has no arguments or keywords.

Defaults

The default state is **service translation**.

Command Modes

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

The **no service translation** command disables mapping between encapsulated ATM PDUs and encapsulated Frame Relay PDUs.

Examples

The following example shows an FRF.8 configuration with service translation disabled:

```
Router# show running-config

Building configuration...

Current configuration:

connect service-1 Serial1/0 16 ATM3/0 1/32 service-interworking
 no service translation
 efci-bit map-fecn
```

The following example shows how to configure service translation on the connection named service-1:

```
Router(config)# connect service-1 serial1/0 16 ATM3/0 1/32 service-interworking
Router(config-frf8)# service translation
```

Related Commands

Command	Description
clp-bit	Sets the ATM CLP field in the ATM cell header.
connect (FRF.5)	Sets the Frame Relay DE bit field in the Frame Relay cell header.
de-bit map-clp	Sets the EFCI bit field in the ATM cell header.

set fr-fecn-becn

To enable forward explicit congestion notification (FECN) and backward explicit congestion notification (BECN) with Frame Relay over MPLS, use the **set fr-fecn-becn** command in policy map class configuration mode. To disable the configuration notification, use the **no** form of this command.

set fr-fecn-becn *percent*

no set fr-fecn-becn *percent*

Syntax Description

percent	Specifies how much (percentage) of the total queue size should be used before marking the FECN and BECN bits. The valid range of percentages is 0 to 99. Setting the threshold to 0 indicates that all traffic is marked with FECN and BECN bits.

Defaults

Frame Relay does not perform FECN and BECN marking.

Command Modes

Policy map class configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(27)SXA	This command was integrated into Cisco IOS Release 12.2(27)SXA.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

This command works only with Frame Relay over MPLS.

If you configure FECN and BECN bit marking, you cannot configure bandwidth or priority.

Examples

The following example enables marking the FECN and BECN bits when 20 percent of the queue is used:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# shape 80000
Router(config-pmap-c)# set fr-fecn-becn 20
```

Related Commands

Command	Description
threshold ecn	Sets the FECN and BECN marking at the interface level.

shape fr-voice-adapt

To enable Frame Relay voice-adaptive traffic shaping, use the **shape fr-voice-adapt** command in policy-map class configuration mode. To disable Frame Relay voice-adaptive traffic shaping, use the **no** form of this command.

shape fr-voice-adapt [**deactivation** *seconds*]

no shape fr-voice-adapt

Syntax Description

deactivation *seconds*	(Optional) Number of seconds that must elapse after the last voice packet is transmitted before the sending rate is increased to the committed information rate (CIR). The range is from 1 to 10000.

Defaults

Frame Relay voice-adaptive traffic shaping is not enabled.
Seconds: 30

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Frame Relay voice-adaptive traffic shaping enables a router to reduce the permanent virtual circuit (PVC) sending rate to the minimum CIR (minCIR) whenever packets (usually voice) are detected in the low latency queueing priority queue or H.323 call setup signaling packets are present. When there are no packets in priority queue and signaling packets are not present for a configured period of time, the router increases the PVC sending rate from minCIR to CIR to maximize throughput.

The **shape fr-voice-adapt** command can be configured only in the class-default class. If you configure the **shape fr-voice-adapt** command in another class, the associated Frame Relay map class will be rejected when you attach it to the interface.

Frame Relay voice-adaptive traffic shaping can be used with other types of adaptive traffic shaping. For example, when both voice-adaptive traffic shaping and adaptive shaping based on interface congestion are configured, the sending rate will change to minCIR if there are packets in the priority queue or the interface queue size exceeds the configured threshold.

Note Although the priority queue is generally used for voice traffic, Frame Relay voice-adaptive traffic shaping will respond to any packets (voice or data) in the priority queue.

In order to use Frame Relay voice-adaptive traffic shaping, you must have low latency queueing and traffic shaping configured using the Modular QoS CLI.

Examples

The following example shows the configuration of Frame Relay voice-adaptive traffic shaping and fragmentation. With this configuration, priority-queue packets or H.323 call setup signaling packets destined for PVC 100 will result in the reduction of the sending rate from CIR to minCIR and the activation of FRF.12 end-to-end fragmentation. If signaling packets and priority-queue packets are not detected for 50 seconds, the sending rate will increase to CIR and fragmentation will be turned off.

```
interface serial0
 encapsulation frame-relay
 frame-relay fragmentation voice-adaptive deactivation 50
 frame-relay fragment 80 end-to-end
 frame-relay interface-dlci 100
  class voice_adaptive_class
!
map-class frame-relay voice_adaptive_class
 frame-relay fair-queue
 service-policy output shape

class-map match-all voice
 match access-group 102
class-map match-all data
 match access-group 101

policy-map vats
 class voice
  priority 10
 class data
  bandwidth 10

policy-map shape
 class class-default
  shape average 60000
  shape adaptive 30000
  shape fr-voice-adapt deactivation 50
  service-policy vats
```

Related Commands

Command	Description
frame-relay fragmentation voice-adaptive	Enables voice-adaptive Frame Relay fragmentation.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either by interface or subinterface or by PVC.

show acircuit checkpoint

To display checkpointing information for each attachment circuit (AC), use the **show acircuit checkpoint** command in privileged EXEC mode.

show acircuit checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used for interface-based attachment circuits. For Frame Relay and ATM circuits, use the following commands to show redundancy information:

- **debug atm ha-error**
- **debug atm ha-events**
- **debug atm ha-state**
- **debug atm l2transport**
- **debug frame-relay redundancy**

Examples

The following **show acircuit checkpoint** command displays information about the ACs that have been check-pointed. The output varies, depending on whether the command output is for the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show acircuit checkpoint

AC HA Checkpoint info:
Last Bulk Sync: 1 ACs
 AC    IW    XC    Id  VCId   Switch    Segment  St  Chkpt
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100      1000      1000   0    N
VLAN  LIKE  ATOM    2  1002      2001      2001   3    Y
```

On the standby RP, the command displays the following output::

```
Router# show acircuit checkpoint

AC HA Checkpoint info:
 AC    IW    XC    Id  VCId   Switch    Segment  St  F-SLP
----  ----  ----  ---  ----  --------  --------  --  -----
HDLC  LIKE  ATOM    3   100         0         0   0   001
VLAN  LIKE  ATOM    2  1002      2001      2001   2   000
```

Table 21 describes the significant fields shown in the display.

Table 21 show acircuit checkpoint Field Descriptions

Field	Description
Last Bulk Sync	The number of ACs that were sent to the backup RP during the last bulk synchronization between the active and backup RPs.
AC	The type of attachment circuit.
IW	The type of interworking, either like-to-like (AToM) or any-to-any (Interworking).
XC	The type of cross-connect. Only AToM ACs are checkpointed.
ID	This field varies, depending on the type of attachment circuit. For Ethernet VLANs, the ID is the VLAN ID. For PPP and High-Level Data Link Control (HDLC), the ID is the AC circuit ID.
VCID	The configured virtual circuit ID.
Switch	An ID used to correlate the control plane and data plane contexts for this virtual circuit (VC). This is an internal value that is not for customer use.
Segment	An ID used to correlate the control plane and data plane contexts for this VC. This is an internal value that is not for customer use.
St	The state of the attachment circuit. This is an internal value that is not for customer use.
Chkpt	Whether the information about the AC was checkpointed.
F-SLP	Flags that provide more information about the state of the AC circuit. These values are not for customer use.

Related Commands

Command	Description
show mpls l2transport vc	Displays AToM status information.
show mpls l2transport vc checkpoint	Displays the status of the checkpointing process for both the active and standby RPs.

show connect (FR-ATM)

To display statistics and other information about Frame-Relay-to-ATM Network Interworking (FRF.5) and Frame Relay-to-ATM Service Interworking (FRF.8) connections, use the **show connect** command in privileged EXEC mode.

show connect [**all** | *element* | **id** *ID* | *name* | **port** *port*]

Syntax Description

all	(Optional) Displays information about all Frame Relay-to-ATM connections.
element	(Optional) Displays information about the specified connection element.
id *ID*	(Optional) Displays information about the specified connection identifier.
name	(Optional) Displays information about the specified connection name.
port *port*	(Optional) Displays information about all connections on an interface.

Defaults

Default state is **show connect all**.

Command Modes

Privileged EXEC

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.

Examples

FRF.5: Examples

The following example displays information about all FRF.5 connections:

```
C3640# show connect all

ID   Name               Segment 1            Segment 2           State
========================================================================
5    network-1          VC-Group network-1   ATM3/0 1/34         UP
```

The following example displays information about the specified FRF.5 connection identifier:

```
Router# show connect id 5

FR/ATM Network Interworking Connection: network-1
  Status    - UP
  Segment 1 - VC-Group network-1
  Segment 2 - ATM3/0 VPI 1 VCI 34
  Interworking Parameters -
    de-bit map-clp
    clp-bit map-de
```

FRF.8: Examples

The following example displays information about the specified FRF.8 connection identifier:

```
Router# show connect id 10

FR/ATM Service Interworking Connection: service-1
  Status    - UP
  Segment 1 - Serial1/0 DLCI 16
  Segment 2 - ATM3/0 VPI 1 VCI 32
Interworking Parameters -
    service translation
    efci-bit 0
    de-bit map-clp
    clp-bit map-de
```

The following example displays information about the FRF.8 connection on an interface:

```
Router# show connect port atm3/0

ID   Name               Segment 1            Segment 2           State
========================================================================
10   service-1         Serial1/0 16         ATM3/0 1/32          UP
```

Table 22 describes the fields seen in these displays.

Table 22 show connect Field Descriptions

Display	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Assigned connection name.
Segment 1 or 2	Frame Relay or ATM interworking segments.
State or Status	Status of the connection, UP, DOWN, or ADMIN DOWN.

Related Commands

Command	Description
connect (FRF.8)	Connects a Frame Relay DLCI to an ATM PVC.
show atm pvc	Displays all ATM PVCs, SVCs, and traffic information.
show frame-relay pvc	Displays statistics about Frame Relay interfaces.

show connection

TTo display the status of interworking connections, use the **show connection** command in privileged EXEC mode.

show connection [**all** | *element* | **id** *startid*-[*endid*]] | **name** *name* | **port** *port*]

Syntax Description

all	(Optional) Displays information about all interworking connections.
element	(Optional) Displays information about the specified connection element.
id	(Optional) Displays information about the specified connection identifier.
startid	Starting connection ID number.
endid	(Optional) Ending connection ID number.
name *name*	(Optional) Displays information about the specified connection name.
port *port*	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet are shown.)

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)T	This command was introduced as **show connect** (FR-ATM).
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all ATM, serial, and Fast Ethernet interworking connections.
12.4(2)T	The command output was modified to add Segment 1 and Segment 2 fields for Segment state and channel ID.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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)SB	This command was updated to display High-Level Data Link Control (HDLC) local switching connections.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows the local interworking connections on a router:

```
Router# show connection

ID   Name               Segment 1            Segment 2           State
=====================================================================
1    conn1          ATM 1/0/0 AAL5 0/100   ATM 2/0/0 AAL5 0/100   UP
2    conn2          ATM 2/0/0 AAL5 0/300   Serial0/1 16           UP
3    conn3          ATM 2/0/0 AAL5 0/400   FA 0/0.1 10            UP
4    conn4          ATM 1/0/0 CELL 0/500   ATM 2/0/0 CELL 0/500   UP
5    conn5          ATM 1/0/0 CELL 100     ATM 2/0/0 CELL 100     UP
```

Table 23 describes the significant fields shown in the display.

Table 23 show connection Field Descriptions

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments: • Interface name and number. • Segment state, interface name and number, and channel ID. Segment state will displays nothing if the segment state is UP, "-" if the segment state is DOWN, and "***Card Removed***" if the segment state is DETACHED. • Type of encapsulation (if any) assigned to the interface. • Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.
State	Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.

Related Commands

Command	Description
connect (L2VPN local switching)	Connects two different or like interfaces on a router.
show atm pvc	Displays the status of ATM PVCs and SVCs.
show frame-relay pvc	Displays the status of Frame Relay interfaces.

show ethernet service evc

To display information about Ethernet virtual connections (EVCs), use the **show ethernet service evc** command in privileged EXEC mode.

show ethernet service evc [**detail** | **id** *evc-id* [**detail**] | **interface** *type number* [**detail**]]

Syntax Description

detail	(Optional) Displays detailed information about service instances or the specified service instance ID or interface.
id	(Optional) Displays EVC information for the specified service.
evc-id	(Optional) String from 1 to 100 characters that identifies the EVC.
interface	(Optional) Displays service instance information for the specified interface.
type	(Optional) Type of interface.
number	(Optional) Number of the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

Examples

Following is sample output from the **show ethernet service evc** command:

```
Router# show ethernet service evc

Identifier                      Type  Act-UNI-cnt Status
BLUE                            P-P       2       Active
PINK                            MP-MP     2       PartiallyActive
PURPLE                          P-P       2       Active
BROWN                           MP-MP     2       Active
GREEN                           P-P       3       Active
YELLOW                          MP-MP     2       PartiallyActive
BANANAS                         P-P       0       InActive
TEST2                           P-P       0       NotDefined
ORANGE                          P-P       2       Active
TEAL                            P-P       0       InActive
```

Table 24 describes the significant fields in the output.

Table 24 show ethernet service evc Field Descriptions

Field	Description
Identifier	EVC identifier.
Type	Type of connection, for example point-to-point (P-P) or multipoint-to-multipoint (MP-MP).
Act-UNI-cnt	Number of active user network interfaces (UNIs).
Status	Availability status of the EVC.

Related Commands

Command	Description
show ethernet instance	Displays information about Ethernet customer service instances.
show ethernet interface	Displays interface-only information about Ethernet customer service instances.

show ethernet service instance

To display information about Ethernet customer service instances, use the **show ethernet service instance** command in privileged EXEC mode.

show ethernet service instance [**detail** | **id** *id* | **interface** *type number* | **policy-map** | **stats**]

Syntax Description

detail	(Optional) Displays detailed information about service instances or the specified service instance ID or interface.
id	(Optional) Displays a specific service instance on an interface that does not map to a VLAN.
id	(Optional) Integer in the range of 1 to 4294967295 that identifies a service instance on an interface that does not map to a VLAN.
interface	(Optional) Displays service instance information for a configured interface.
type	(Optional) Type of interface.
number	(Optional) Number of the interface.
policy-map	(Optional) Displays the policy map for the service instance.
stats	(Optional) Displays service instance statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

Examples

Following is an example of output from the **show ethernet service instance** command:

```
Router# show ethernet service instance

Identifier Interface             CE-Vlans
222        FastEthernet0/1       untagged,1-4094
10         FastEthernet0/2
222        FastEthernet0/2       200
333        FastEthernet0/2       default
10         FastEthernet0/3       300
11         FastEthernet0/3
10         FastEthernet0/4       300
10         FastEthernet0/6       untagged,1-4094
10         FastEthernet0/7       untagged,1-4094
10         FastEthernet0/8       untagged,1-4094
10         FastEthernet0/9       untagged
20         FastEthernet0/9
222        FastEthernet0/11      300-350,900-999
333        FastEthernet0/11      100-200,1000,1999-4094
```

```
222         FastEthernet0/12      20
333         FastEthernet0/12      10
10          FastEthernet0/13      10
20          FastEthernet0/13      20
30          FastEthernet0/13      30
200         FastEthernet0/13      222
200         FastEthernet0/14      200,222
300         FastEthernet0/14      333
555         FastEthernet0/14      555
```

Table 25 describes the significant fields in the output.

Table 25 show ethernet service instance Field Descriptions

Field	Description
Identifier	Service instance identifier.
Interface	Interface type and number with which the service instance is associated.
CE-Vlans	Customer edge (CE) device VLAN ID.

Related Commands

Command	Description
show ethernet evc	Displays information about Ethernet customer service instances.
show ethernet interface	Displays interface-only information about Ethernet customer service instances.

show ethernet service interface

To display interface-only information about Ethernet customer service instances for all interfaces or for a specified interface, use the **show ethernet service interface** privileged EXEC mode.

show ethernet service interface [*type number*] [**detail**]

Syntax Description

type	(Optional) Type of interface.
number	(Optional) Number of the interface.
detail	(Optional) Displays detailed information about interfaces or a specified service instance ID or interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEG	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that contain "Output" are displayed.

Examples

Following are examples of output from the **show ethernet service interface** command:

```
Router# show ethernet service interface gigabitethernet0/1

Interface          Identifier
GigabitEthernet0/1 PE2-G101

Router# show ethernet service interface detail

Interface: FastEthernet0/1
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/2
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing
Interface: FastEthernet0/3
ID:
CE-VLANS:
EVC Map Type: Bundling-Multiplexing

<output truncated>

Interface: GigabitEthernet0/1
ID: PE2-G101
CE-VLANS: 10,20,30
```

```
EVC Map Type: Bundling-Multiplexing
Associated EVCs:
EVC-ID CE-VLAN
WHITE 30
RED 20
BLUE 10
Associated Service Instances:
Service-Instance-ID CE-VLAN
10 10
20 20
30 30
```

Table 26 describes the significant fields in the output.

Table 26 show ethernet service interface Field Descriptions

Field	Description
Interface	Interface type and number.
Identifier	EVC identifier.
ID	EVC identifier.
CE-VLANS	VLANs associated with the customer edge (CE) device.
EVC Map Type	UNI service type; for example, Bundling, Multiplexing, All-to-one Bundling.
Associated EVCs	EVCs associated with a device.
EVC-ID CE-VLAN	EVC identifier and associated VLAN.
Associated Service Instances	Service instances associated with a device.
Service-Instance-ID CE-VLAN	Service instance identifier and its associated CE VLAN.

Related Commands

Command	Description
service instance ethernet	Defines an Ethernet service instance and enters Ethernet service configuration mode.
show ethernet evc	Displays information about Ethernet customer service instances.
show ethernet interface	Displays interface-only information about Ethernet customer service instances.

show flow monitor type mace

To display the status and statistics for a flow monitor of type Measurement, Aggregation, and Correlation Engine (MACE), use the **show flow monitor type mace** command in privileged EXEC mode.

show flow monitor type mace [*name*]

Syntax Description

name	(Optional) Name of a specific MACE flow monitor that is configured using the **flow monitor type mace** command.

Command Default

If no flow monitor name is specified, the command displays the status and statistics of all the configured flow monitors of type MACE.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show flow monitor type** command to display the status and statistics for a flow monitor of type MACE. If no flow monitor name is specified, the command displays the status and statistics of all the configured flow monitors of type MACE.

Note You need to configure the **flow monitor type mace** command with a specific name to display the output for that flow monitor name using this command.

Examples

The following is sample output from the **show flow monitor type mace** command:

```
Router# show flow monitor type mace mace_monitor_1

Flow Monitor type mace mace_monitor_1:
Description: User defined
Flow Record: mace_record
Flow Exporter: mace_exporter
No. of Inactive Users: 1
No. of Active Users: 0
Cache Timeout Update: 2 seconds
```

Table 27 describes the significant fields shown in the display.

Table 27 show flow record type mace Field Descriptions

Field	Description
Description	Displays the description provided for a flow monitor.
Flow Record	Displays the flow record that is included in the flow monitor.
Flow Exporter	Displays the flow exporter that is included in the flow monitor.
No. of Inactive Users	Displays the number of times that a flow monitor is inactive.
No. of Active Users	Displays the number of times that a flow monitor is active as an action under a policy when the policy is applied under an interface.
Cache Timeout Update	Displays the frequency with which the cache timeout is updated.

Related Commands

Command	Description
cache (Flexible NetFlow)	Configures a flow cache parameter for a Flexible NetFlow flow monitor.
flow monitor type mace	Configures a flow monitor of type MACE.
flow record	Configures the status and statistics for a Flexible Netflow flow record.

show flow record type

To display the configuration for a flow record, use the **show flow record type** command in privileged EXEC mode.

show flow record type {**mace** [[**name**] *flow-record-name*] | **performance-monitor** [**name**] [**default-rtp** | **default-tcp** | *record-name*]}

Syntax Description

mace	Displays Measurement, Aggregation, and Correlation Engine (MACE) metrics for the flow record.
name	(Optional) Displays the configuration for a specific MACE flow record if it is used with the **mace** keyword. Displays the configuration for a specific performance monitor flow record if it is used with the **performance-monitor** keyword.
flow-record-name	(Optional) Name of the user-defined MACE flow record that was previously configured.
performance-monitor	Displays configuration for the flow record of type performance monitor.
default-rtp	(Optional) Displays the Video Monitoring (VM) default Real-time Transport Protocol (RTP) record.
default-tcp	(Optional) Displays the VM default TCP record.
record-name	(Optional) Name of the user-defined performance monitor that was previously configured.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show flow record type** command to display the status and statistics for various flow record types. If you chose to use the **name** keyword in the command, you must use either the **default-rtp** or **default-tcp** keywords, or use the *record-name* argument to complete the command.

Note You need to configure a flow record of type MACE using the **flow record type mace** command in order for the output of the **show flow record type mace** command to display information about the configured flow record.

Note You need to configure a flow record of type performance monitor using the **flow record type performance-monitor** command in order for the output of the **show flow record type performance-monitor** command to display information about the configured flow record.

Examples

The following is sample output from the **show flow record type mace** command:

```
Router# show flow record type mace mace1

flow record type mace mace1:
  Description:        User defined
  No. of users:       0
  Total field space:  164 bytes
  Fields:
    collect art all
```

The following is sample output from the **show flow record type performance-monitor** command:

```
Router# show flow record type performance-monitor p1

flow record type performance-monitor p1:
  Description:        User defined
  No. of users:       0
  Total field space:  4 bytes
  Fields:
    collect application media bytes rate
```

Table 28 describes the significant fields shown in the above examples.

Table 28 show flow record type Field Descriptions

Field	Description
Description	Provides a description for this flow record.
No. of users	Indicates how many times a particular flow record has been used under a flow monitor.
Total field space	Displays the size of the record in bytes.
Fields	Displays the names of the fields that are configured.

Related Commands

Command	Description
flow record	Configures the status and statistics for an Flexible NetFlow flow record.
flow record type mace	Configures a flow record for MACE.
flow record type performance monitor	Configures a flow record for performance monitor.

show frame-relay end-to-end keepalive

To display statistics about Frame Relay end-to-end keepalive, use the **show frame-relay end-to-end keepalive** command in privileged EXEC mode.

show frame-relay end-to-end keepalive [*interface* [*dlci*] | *failures*]

Syntax Description

interface	(Optional) Interface to display.
dlci	(Optional) DLCI to display.
failures	(Optional) Displays the number of times keepalive has failed and the elapsed time since the last failure occurred.

Defaults

If no interface is specified, show all interfaces.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4T	This command was modified for Cisco IOS Release 12.4T.
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 display the keepalive status of an interface.

Examples

The following examples show output from the **show frame-relay end-to-end keepalive** command:

Displaying Statistics About Frame Relay End-to-End Keepalive: Example

```
Router# show frame-relay end-to-end keepalive interface s1

End-to-end Keepalive Statistics for Interface Serial1 (Frame Relay DTE)
DLCI = 100, DLCI USAGE = LOCAL, VC STATUS = STATIC (EEK UP)

SEND SIDE STATISTICS
Send Sequence Number: 86,       Receive Sequence Number: 87
Configured Event Window: 3,     Configured Error Threshold: 2
Total Observed Events: 90,      Total Observed Errors: 34
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP

RECEIVE SIDE STATISTICS
Send Sequence Number: 88,       Receive Sequence Number: 87
Configured Event Window: 3,     Configured Error Threshold: 2
```

```
Total Observed Events: 90,      Total Observed Errors: 33
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP
```

Displaying Failure Statistics About Frame Relay End-to-End Keepalive: Example

```
Router# show frame-relay end-to-end keepalive interface s1 failures

End-to-end Keepalive Statistics for Interface Serial1 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, VC STATUS = STATIC (EEK UP)

SEND SIDE STATISTICS

Send Sequence Number: 86,       Receive Sequence Number: 87
Configured Event Window: 3,     Configured Error Threshold: 2
Total Observed Events: 90,      Total Observed Errors: 34
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP

RECEIVE SIDE STATISTICS

Send Sequence Number: 88,       Receive Sequence Number: 87
Configured Event Window: 3,     Configured Error Threshold: 2
Total Observed Events: 90,      Total Observed Errors: 33
Monitored Events: 3,            Monitored Errors: 0
Successive Successes: 3,        End-to-end VC Status: UP

Failures Since Started: 1,      Last Failure: 00:01:31
```

Table 29 describes the fields shown in the display.

Table 29 show frame-relay end-to-end keepalive Field Descriptions

Field	Description
DLCI	The DLCI number that identifies the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.

Table 29 show frame-relay end-to-end keepalive Field Descriptions (continued)

Field	Description
VC STATUS	Status of the PVC. The DCE device reports the status, and the DTE device receives the status. When you disable the Local Management Interface (LMI) mechanism on the interface (by using the no keepalive command), the PVC status is STATIC. Otherwise, the PVC status is exchanged using the LMI protocol: • STATIC—LMI is disabled on the interface. • ACTIVE— The PVC is operational and can transmit packets. • INACTIVE—The PVC is configured, but down. • DELETED—The PVC is not present (DTE device only), which means that no status is received from the LMI protocol. If the frame-relay end-to-end keepalive command is used, the end-to-end keepalive (EEK) status is reported in addition to the LMI status. For example: • ACTIVE (EEK UP) —The PVC is operational according to LMI and end-to-end keepalives. • ACTIVE (EEK DOWN)—The PVC is operational according to LMI, but end-to-end keepalive has failed.
Send Sequence Number	The current sequence number being sent in the keepalive packets.
Receive Sequence Number	The last sequence number received in the incoming keepalive packets.
Configured Event Window	The value configured by frame-relay end-to-end keepalive event-window command.
Configured Error Threshold	The value configured by frame-relay end-to-end keepalive error-threshold command.
Total Observed Events	The total number of successful events counted.
Total Observed Errors	The total number of error events counted.
Monitored Events	The number of events in current event window.
Monitored Errors	The number of errors in current event window.
Successive Successes	The number of successive success events in the current event window.
End-to-end VC Status	The status of the end-to-end keepalive protocol. The status is either UP or DOWN.
Failures Since Started	The number of times the end-to-end keepalive protocol has failed, causing the DLCI to go into the EEK DOWN state, since the protocol started.
Last Failure	The elapsed time since the last failure.

Related Commands

Command	Description
frame-relay end-to-end keepalive error-threshold	Modifies the keepalive error threshold value.
frame-relay end-to-end keepalive event-window	Modifies the keepalive event window value.
frame-relay end-to-end keepalive mode	Enables Frame Relay end-to-end keepalives.
frame-relay end-to-end keepalive success-events	Modifies the keepalive success events value.

Command	Description
frame-relay end-to-end keepalive timer	Modifies the keepalive timer.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.

show frame-relay fragment

To display information about the Frame Relay fragmentation, use the **show frame-relay fragment** command in privileged EXEC mode.

show frame-relay fragment [**interface** *interface* [*dlci*]]

Syntax Description

interface	(Optional) Indicates a specific interface for which Frame Relay fragmentation information will be displayed.
interface	(Optional) Interface number containing the DLCI(s) for which you wish to display fragmentation information.
dlci	(Optional) Specific DLCI for which you wish to display fragmentation information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)T	This command was introduced.
12.1(2)E	Support was added for Cisco 7500 series routers with Versatile Interface Processors.
12.1(5)T	Support was added for Cisco 7500 series routers with Versatile Interface Processors running 12.1(5)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 no parameters are specified with this command, the output displays a summary of each data-link connection identifier (DLCI) configured for fragmentation. The information displayed includes the fragmentation type, the configured fragment size, and the number of fragments transmitted, received, and dropped.

When a specific interface and DLCI are specified, additional details are displayed.

Examples

The following is sample output for the **show frame-relay fragment** command without any parameters specified:

```
Router# show frame-relay fragment

interface         dlci  frag-type    frag-size  in-frag    out-frag   dropped-frag
Serial0           108   VoFR-cisco   100        1261       1298       0
Serial0           109   VoFR         100        0          243        0
Serial0           110   end-to-end   100        0          0          0
```

The following is sample output for the **show frame-relay fragment** command when an interface and DLCI are specified:

```
Router# show frame-relay fragment interface Serial1/0 16

  fragment-size 45                  fragment type end-to-end
  in fragmented pkts 0              out fragmented pkts 0
  in fragmented bytes 0             out fragmented bytes 0
  in un-fragmented pkts 0           out un-fragmented pkts 0
  in un-fragmented bytes 0          out un-fragmented bytes 0
  in assembled pkts 0               out pre-fragmented pkts 0
  in assembled bytes 0              out pre-fragmented bytes
  in dropped reassembling pkts 0    out dropped fragmenting pkts 0
  in timeouts 0
  in out-of-sequence fragments 0
  in fragments with unexpected B bit set 0
  out interleaved packets 0
```

Table 30 describes the fields shown in the display.

Table 30 show frame-relay fragment Field Descriptions

Field	Description
interface	Subinterface containing the DLCI for which the fragmentation information pertains.
dlci	Data-link connection identifier for which the displayed fragmentation information applies.
frag-type	Type of fragmentation configured on the designated DLCI. Supported types are end-to-end, VoFR, and VoFR-cisco.
frag-size	Configured fragment size in bytes.
in-frag	Total number of fragments received by the designated DLCI.
out-frag	Total number of fragments sent by the designated DLCI.
dropped-frag	Total number of fragments dropped by the designated DLCI.
in/out fragmented pkts	Total number of frames received/sent by this DLCI that have a fragmentation header.
in/out fragmented bytes	Total number of bytes, including those in the Frame Relay headers, that have been received/sent by this DLCI.
in/out un-fragmented pkts	Number of frames received/sent by this DLCI that do not require reassembly, and therefore do not contain the FRF.12 header. These counters can be incremented only when the end-to-end fragmentation type is set.
in/out un-fragmented bytes	Number of bytes received/sent by this DLCI that do not require reassembly, and therefore do not contain the FRF.12 header. These counters can be incremented only when the end-to-end fragmentation type is set.
in assembled pkts	Total number of fully reassembled frames received by this DLCI, including the frames received without a Frame Relay fragmentation header (in unfragmented packets). This counter corresponds to the frames viewed by the upper-layer protocols.

Table 30 show frame-relay fragment Field Descriptions (continued)

Field	Description
out pre-fragmented pkts	Total number of fully reassembled frames transmitted by this DLCI, including the frames transmitted without a Frame Relay fragmentation header (out un-fragmented pkts).
in assembled bytes	Number of bytes in the fully reassembled frames received by this DLCI, including the frames received without a Frame Relay fragmentation header (in un-fragmented bytes). This counter corresponds to the total number of bytes viewed by the upper-layer protocols.
out pre-fragmented bytes	Number of bytes in the fully reassembled frames transmitted by this DLCI, including the frames sent without a Frame Relay fragmentation header (out un-fragmented bytes). This counter corresponds to the total number of bytes viewed by the upper-layer protocols.
in dropped reassembling pkts	Number of fragments received by this DLCI that are dropped for reasons such as running out of memory, receiving segments out of sequence, receiving an unexpected frame with a B bit set, or timing out on a reassembling frame.
out dropped fragmenting pkts	Number of fragments that are dropped by this DLCI during transmission because of running out of memory.
in timeouts	Number of reassembly timeouts that have occurred on incoming frames to this DLCI. (A frame that does not fully reassemble within two minutes is dropped, and the timeout counter is incremented.)
in out-of-sequence fragments	Number of fragments received by this DLCI that have an unexpected sequence number.
in fragments with unexpected B bit set	Number of fragments received by this DLCI that have an unexpected B bit set. When this occurs, all fragments being reassembled are dropped and a new frame is begun with this fragment.
out interleaved packets	Number of packets leaving this DLCI that have been interleaved between segments.

Related Commands

Command	Description
frame-relay fragment	Enables fragmentation of Frame Relay frames for a Frame Relay map class.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.
show interfaces serial	Displays information about a serial interface.
show traffic-shape queue	Displays information about the elements queued at a particular time at the VC level.

show frame-relay iphc

To display Frame Relay IP Header Compression Implementation Agreement (FRF.20) negotiation parameters for each PVC, use the **show frame-relay iphc** command in user EXEC or privileged EXEC mode.

show frame-relay iphc [**interface** *interface*] [*dlci*]

Syntax Description

interface	(Optional) Indicates a specific interface for which Frame Relay fragmentation information will be displayed.
interface	(Optional) Interface number containing the data link connection identifiers (DLCI(s)) for which you wish to display fragmentation information.
dlci	(Optional) Specific Data-Link Connection Identifier (DLCI) for which you wish to display fragmentation information. Valid values are from 16 to 1022.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.1(2)E	This command was integrated into Cisco IOS Release 12.1(2)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.

Examples

The following is sample output for the **show frame-relay iphc** command without any parameters specified:

```
Router# show frame-relay iphc

FRF.20 Statistics for Interface Serial2/0

DLCI 16 :
Parameters:        TCP space  16     non TCP space  16
F_MAX period  256  F_MAX time 5      MAX header     168

CP: State - req sent CP drops  0
Reqs txed   2        Req rxed  0      Acks txed   0      Acks rxed  0
```

Table 31 describes the significant fields shown in the display.

Table 31 show frame-relay iphc Field Descriptions

Field	Description
DLCI	The DLCI number that identifies the PVC.

Table 31 show frame-relay iphc Field Descriptions (continued)

Field	Description
Parameters	Indicates FRF negotiation parameters configured for PVCs.
CP: State	Indicates the status of control protocol frames.

Related Commands

Command	Description
frame-relay fragment	Enables fragmentation of Frame Relay frames for a Frame Relay map class.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.
show interfaces serial	Displays information about a serial interface.
show traffic-shape queue	Displays information about the elements queued at a particular time at the VC level.

show frame-relay ip tcp header-compression

To display Frame Relay Transmission Control Protocol (TCP)/IP header compression statistics, use the **show frame-relay ip tcp header-compression** command in user EXEC or privileged EXEC mode.

show frame-relay ip tcp header-compression [**interface** *type number*] [*dlci*]

Syntax Description

interface *type number*	(Optional) Specifies an interface for which information will be displayed. A space is optional between the type and number.
dlci	(Optional) Specifies a data-link connection identifier (DLCI) for which information will be displayed. Range is from 16 to 1022.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The command was modified to support display of RTP header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC, and the *dlci* argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(9)T	The *dlci* argument was 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.

Examples

The following is sample output from the **show frame-relay ip tcp header-compression** command:

```
Router# show frame-relay ip tcp header-compression

DLCI 200          Link/Destination info: ip 10.108.177.200
Interface Serial0:
Rcvd:     40 total, 36 compressed, 0 errors
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     0 total, 0 compressed
          0 bytes saved, 0 bytes sent
Connect:  16 rx slots, 16 tx slots, 0 long searches, 0 misses, 0% hit ratio
          Five minute miss rate 0 misses/sec, 0 max misses/sec
```

The following sample output from the **show frame-relay ip tcp header-compression** command shows statistics for a PVC bundle called “MP-3-static”:

```
Router# show frame-relay ip tcp header-compression interface Serial1/4

 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
             474 bytes saved, 119 bytes sent
             4.98 efficiency improvement factor
    Connect:256 rx slots, 256 tx slots,
             1 long searches, 1 misses 0 collisions, 0 negative cache hits
             93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

In the following example, the **show frame-relay ip tcp header-compression** command displays information about DLCI 21:

```
Router# show frame-relay ip tcp header-compression 21

DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts

DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following is sample output from the **show frame-relay ip tcp header-compression** command for a specific DLCI on a specific interface:

```
Router# show frame-relay ip tcp header-compression pos2/0 21

DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

Table 32 describes the fields shown in the display.

Table 32 show frame-relay ip tcp header-compression Field Descriptions

Field	Description
Rcvd:	Table of details concerning received packets.
total	Sum of compressed and uncompressed packets received.

Table 32 show frame-relay ip tcp header-compression Field Descriptions (continued)

Field	Description
compressed	Number of compressed packets received.
errors	Number of errors caused by errors in the header fields (version, total length, or IP checksum).
dropped	Number of packets discarded. Seen only after line errors.
buffer failures	Number of times that a new buffer was needed but was not obtained.
Sent:	Table of details concerning sent packets.
total	Sum of compressed and uncompressed packets sent.
compressed	Number of compressed packets sent.
bytes saved	Number of bytes reduced because of the compression.
bytes sent	Actual number of bytes transmitted.
Connect:	Table of details about the connections.
rx slots, tx slots	Number of states allowed over one TCP connection. A state is recognized by a source address, a destination address, and an IP header length.
long searches	Number of times that the connection ID in the incoming packet was not the same as the previous one that was processed.
misses	Number of times that a matching entry was not found within the connection table and a new entry had to be entered.
hit ratio	Percentage of times that a matching entry was found in the compression tables and the header was compressed.
Five minute miss rate	Miss rate computed over the most recent 5 minutes and the maximum per-second miss rate during that period.

show frame-relay lapf

To display information about the status of the internals of Frame Relay Layer 2 (LAPF) if switched virtual circuits (SVCs) are configured, use the **show frame-relay lapf** command in user EXEC or privileged EXEC mode.

show frame-relay lapf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
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.

Examples

The following is sample output from the **show frame-relay lapf** command.

```
Router# show frame-relay lapf

Interface = Serial1 (up),  LAPF state = TEI_ASSIGNED (down)
SVC disabled, link down cause = LMI down,  #link-reset = 0
T200 = 1.5 sec.,  T203 = 30 sec.,  N200 = 3,  k = 7,  N201 = 260
I xmt = 0, I rcv = 0, I reXmt = 0, I queued = 0
I xmt dropped = 0,  I rcv dropped = 0,  Rcv pak dropped = 0
RR xmt = 0,  RR rcv = 0,  RNR xmt = 0,  RNR rcv = 0
REJ xmt = 0,  REJ rcv = 0,  FRMR xmt = 0,  FRMR rcv = 0
DM xmt = 0,  DM rcv = 0,  DISC xmt = 0,  DISC rcv = 0
SABME xmt = 0,  SABME rcv = 0,  UA xmt = 0,  UA rcv = 0
V(S) = 0,  V(A) = 0,  V(R) = 0,  N(S) = 0,  N(R) = 0
Xmt FRMR at Frame Reject
```

Table 33 describes significant fields in this output.

Table 33 show frame-relay lapf Field Descriptions

Field	Description
Interface	Identifies the interface and indicates the line status (up, down, administratively down).
LAPF state	A LAPF state of MULTIPLE FRAME ESTABLISHED or RIMER_RECOVERY indicates that Layer 2 is functional. Others, including TEI_ASSIGNED, AWAITING_ESTABLISHMENT, and AWAITING_RELEASE, indicate that Layer 2 is not functional.

Table 33 show frame-relay lapf Field Descriptions (continued)

Field	Description
SVC disabled	Indicates whether SVCs are enabled or disabled.
link down cause	Indicates the reason that the link is down. For example, N200 error, memory out, peer disconnect, LMI down, line down, and SVC disabled. Many other causes are described in the Q.922 specification.
#link-reset	Number of times the Layer 2 link has been reset.
T200, T203, N200, k, N201	Values of Layer 2 parameters.
I xmt, I rcv, I reXmt, I queued	Number of I frames sent, received, retransmitted, and queued for transmission, respectively.
I xmt dropped	Number of sent I frames that were dropped.
I rcv dropped	Number of I frames received over DLCI 0 that were dropped.
Rcv pak dropped	Number of received packets that were dropped.
RR xmt, RR rcv	Number of RR frames sent; number of RR frames received.
RNR xmt, RNR rcv	Number of RNR frames sent; number of RNR frames received.
REJ xmt, REJ rcv	Number of REJ frames sent; number of REJ frames received.
FRMR xmt, FRMR rcv	Number of FRMR frames sent; number of FRMR frames received.
DM xmt, DM rcv	Number of DM frames sent; number of DM frames received.
DISC xmt, DISC rcv	Number of DISC frames sent; number of DISC frames received.
SABME xmt, SABME rcv	Number of SABME frames sent; number of SABME frames received.
UA xmt, UA rcv	Number of UA frames sent; number of UA frames received.
V(S) 0, V(A) 0, V(R) 0, N(S) 0, N(R) 0	Layer 2 sequence numbers.
Xmt FRMR at Frame Reject	Indicates whether the FRMR frame is sent at Frame Reject.

show frame-relay lmi

To display statistics about the Local Management Interface (LMI), use the **show frame-relay lmi** command in user EXEC or privileged EXEC mode.

show frame-relay lmi [*type number*]

Syntax Description

type	(Optional) Interface type; it must be **serial**.
number	(Optional) Interface number.

Command Modes

User EXEC
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.

Usage Guidelines

Enter the command without arguments to obtain statistics about all Frame Relay interfaces.

Examples

The following is sample output from the **show frame-relay lmi** command when the interface is a data terminal equipment (DTE) device:

```
Router# show frame-relay lmi

LMI Statistics for interface Serial1 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Sent 9                Num Status msgs Rcvd 0
  Num Update Status Rcvd 0              Num Status Timeouts 9
```

The following is sample output from the **show frame-relay lmi** command when the interface is a Network-to-Network Interface (NNI):

```
Router# show frame-relay lmi

LMI Statistics for interface Serial3 (Frame Relay NNI) LMI TYPE = CISCO
  Invalid Unnumbered info 0             Invalid Prot Disc 0
  Invalid dummy Call Ref 0              Invalid Msg Type 0
  Invalid Status Message 0              Invalid Lock Shift 0
  Invalid Information ID 0              Invalid Report IE Len 0
  Invalid Report Request 0              Invalid Keep IE Len 0
  Num Status Enq. Rcvd 11               Num Status msgs Sent 11
```

```
Num Update Status Rcvd 0              Num St Enq. Timeouts 0
Num Status Enq. Sent 10               Num Status msgs Rcvd 10
Num Update Status Sent 0              Num Status Timeouts 0
```

Table 34 describes significant fields shown in the output.

Table 34 show frame-relay lmi Field Descriptions

Field	Description
LMI Statistics	Signalling or LMI specification: CISCO, ANSI, or ITU-T.
Invalid Unnumbered info	Number of received LMI messages with invalid unnumbered information field.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.
Invalid dummy Call Ref	Number of received LMI messages with invalid dummy call references.
Invalid Msg Type	Number of received LMI messages with invalid message type.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length.
Invalid Report Request	Number of received LMI messages with invalid Report Request.
Invalid Keep IE Len	Number of received LMI messages with invalid Keep IE Length.
Num Status Enq. Sent	Number of LMI status inquiry messages sent.
Num Status Msgs Rcvd	Number of LMI status messages received.
Num Update Status Rcvd	Number of LMI asynchronous update status messages received.
Num Status Timeouts	Number of times the status message was not received within the keepalive time value.
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Status Msgs Sent	Number of LMI status messages sent.
Num Status Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.
Num Update Status Sent	Number of LMI asynchronous update status messages sent.

show frame-relay map

To display current Frame Relay map entries and information about connections, use the **show frame-relay map** command in privileged EXEC mode.

show frame-relay map [**interface** *type number*] [*dlci*]

Syntax Description

interface *type number*	(Optional) Specifies an interface for which mapping information will be displayed. A space is optional between the interface type and number.
dlci	(Optional) Specifies a data-link connection identifier (DLCI) for which mapping information will be displayed. Range: 16 to 1022.

Command Default

Static and dynamic Frame Relay map entries and information about connections for all DLCIs on all interfaces are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(2)T	The display output for this command was modified to include the IPv6 address mappings of remote nodes to Frame Relay permanent virtual circuits (PVCs).
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The display output for this command was modified to include information about Frame Relay PVC bundle maps.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, the **interface** keyword was added, and the *dlci* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The **interface** keyword was added, and the *dlci* argument was added.
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

This section contains the following examples:

- Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example, page 430
- Display Maps for PVC Bundles: Example, page 431
- Display Maps for IPv6 Addresses: Example, page 432

Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example

The sample output in these examples uses the following configuration:

```
interface POS2/0
 no ip address
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 20 tcp header-compression
 frame-relay map ip 10.1.2.1 21 tcp header-compression
 frame-relay map ip 10.1.3.1 22 tcp header-compression
 frame-relay map bridge 23
 frame-relay interface-dlci 25
 frame-relay interface-dlci 26
 bridge-group 1
interface POS2/0.1 point-to-point
 frame-relay interface-dlci 24 protocol ip 10.1.4.1

interface Serial3/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay map ip 172.16.3.1 20
 frame-relay map ip 172.16.4.1 21 tcp header-compression active
 frame-relay map ip 172.16.1.1 100
 frame-relay map ip 172.16.2.1 101
interface Serial3/0.1 multipoint
 frame-relay map ip 192.168.11.11 24
 frame-relay map ip 192.168.11.22 105
```

The following example shows how to display all maps:

```
Router# show frame-relay map

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
              CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
Serial3/0 (downup): ip 172.16.3.1 dlci 20(0x14,0x440), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.4.1 dlci 21(0x15,0x450), static,
              CISCO, status deleted
              TCP/IP Header Compression (enabled), connections: 256
Serial3/0.1 (downup): ip 192.168.11.11 dlci 24(0x18,0x480), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.1.1 dlci 100(0x64,0x1840), static,
              CISCO, status deleted
Serial3/0 (downup): ip 172.16.2.1 dlci 101(0x65,0x1850), static,, CISCO,
              CISCO, status deleted
              ECRTP Header Compression (enabled, IETF), connections 16
              TCP/IP Header Compression (enabled, IETF), connections 16
Serial3/0.1 (downup): ip 192.168.11.22 dlci 105(0x69,0x1890), static,
              CISCO, status deleted
Serial4/0/1:0.1 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast, CISCO
          status defined, active,
              RTP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific DLCI:

```
Router# show frame-relay map 20

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
Serial3/0 (down): ip 172.16.3.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
```

The following example shows how to display maps for a specific interface:

```
Router# show frame-relay map interface pos2/0

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
             CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

The following example shows how to display maps for a specific DLCI on a specific interface:

```
Router# show frame-relay map interface pos2/0 20

POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1

POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

The following example shows how to display maps for a specific DLCI on a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1 24

POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
          status deleted
```

Display Maps for PVC Bundles: Example

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 ip address 30.0.0.2 255.255.255.0
 encapsulation frame-relay
 frame-relay vc-bundle vcb1
  pvc 100 vcb1-classA
   precedence 1-7
   class vcb1-classA
  pvc 109 vcb1-others
   precedence other
   class others
```

```
 frame-relay intf-type dce
!
map-class frame-relay vcb1-classA
 frame-relay cir 128000
!
map-class frame-relay others
 frame-relay cir 64000

hostname router2
!
interface Serial3/3
 ip address 30.0.0.1 255.255.255.0
 encapsulation frame-relay
 frame-relay vc-bundle vcb1
  pvc 100 vcb1-classA
   precedence 1-7
   class vcb1-classA
  pvc 109 vcb1-others
   precedence other
   class others
!
map-class frame-relay vcb1-classA
 frame-relay cir 128000
!
map-class frame-relay others
 frame-relay cir 64000
```

The following sample output displays mapping information for two PVC bundles. The PVC bundle MAIN-1-static is configured with a static map. The map for PVC bundle MAIN-2-dynamic is created dynamically using Inverse Address Resolution Protocol (ARP).

```
Router# show frame-relay map

Serial1/4 (up): ip 10.1.1.1 vc-bundle MAIN-1-static, static,
          CISCO, status up
Serial1/4 (up): ip 10.1.1.2 vc-bundle MAIN-2-dynamic, dynamic,
          broadcast, status up
```

Display Maps for IPv6 Addresses: Example

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 no ip address
 encapsulation frame-relay
!
interface Serial2/0.1 point-to-point
 ipv6 address 1::1/64
 frame-relay interface-dlci 101
!
interface Serial2/0.2 multipoint
 ipv6 address 2::1/64
 frame-relay map ipv6 2::2 201
 frame-relay interface-dlci 201
!

hostname router2
!
interface Serial3/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
```

```
!
interface Serial3/3.1 point-to-point
 ipv6 address 1::2/64
 frame-relay interface-dlci 101
!
interface Serial3/3.2 multipoint
 ipv6 address 2::2/64
 frame-relay map ipv6 3::1 201
 frame-relay interface-dlci 201
!
```

The following sample output from the **show frame-relay map** command shows that the link-local and global IPv6 addresses (FE80::E0:F727:E400:A and 2001:0DB8:2222:1044::32; FE80::60:3E47:AC8:8 and 2001:0DB8:2222:1044::32) of two remote nodes are explicitly mapped to DLCI 17 and DLCI 19, respectively. Both DLCI 17 and DLCI 19 are terminated on interface serial 3 of this node; therefore, interface serial 3 of this node is a point-to-multipoint interface.

```
Router# show frame-relay map

Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,
              broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 19(0x13,0x430), static,
              CISCO, status defined, active

Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 17(0x11,0x410), static,
              CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
              broadcast, CISCO, status defined, active
```

Table 35 describes the significant fields shown in the displays.

Table 35 show frame-relay map Field Descriptions

Field	Description
POS2/0 (up)	Identifies a Frame Relay interface and its status (up or down).
ip 10.1.1.1	Destination IP address.
dlci 20(0x14,0x440)	DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (20), its hexadecimal value (0x14), and its value as it would appear on the wire (0x440).
vc-bundle	PVC bundle that serves as the logical connection being used to reach the interface.
static/dynamic	Indicates whether this is a static or dynamic entry.
broadcast	Indicates pseudobroadcasting.
CISCO	Indicates the encapsulation type for this map: either CISCO or IETF.

Table 35 show frame-relay map Field Descriptions (continued)

Field	Description
TCP/IP Header Compression (inherited), passive (inherited)	Indicates the header compression type (TCP/IP, Real-Time Transport Protocol (RTP), or Enhanced Compressed Real-Time Transport Protocol (ECRTP)) and whether the header compression characteristics were inherited from the interface or were explicitly configured for the IP map.
status defined, active	Indicates that the mapping between the destination address and the DLCI used to connect to the destination address is active.

Related Commands

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vc-bundle	Displays attributes and other information about a Frame Relay PVC bundle.

show frame-relay multilink

To display configuration information and statistics about multilink Frame Relay bundles and bundle links, use the **show frame-relay multilink** command in user EXEC or privileged EXEC mode.

show frame-relay multilink [**mfr** *number* | **serial** *number*] [**dlci** {*dlci-number* | **lmi**}] [**detailed**]

Syntax Description

mfr *number*	(Optional) Displays information about a specific bundle interface.
serial *number*	(Optional) Displays information about a specific bundle link interface.
dlci	(Optional) Displays information about the data-link connection identifier (DLCI).
dlci-number	DLCI number. The range is from 16 to 1022.
lmi	Displays information about the Local Management Interface (LMI) DLCI.
detailed	(Optional) Displays more-detailed information, including counters for the control messages sent to and from the peer device and the status of the bundle links.

Command Default

Information for all bundles and bundle links is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.0(30)S	This command was updated to display Multilink Frame Relay variable bandwidth class status.
12.4(2)T	This command was updated to display Multilink Frame Relay variable bandwidth class status.
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 was integrated into 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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Examples

All Bundles and Bundle Links: Example

The following is sample output from the **show frame-relay multilink** command (see Table 36 for descriptions of the fields). Because a specific bundle or bundle link is not specified, information for all bundles and bundle links is displayed:

```
Router# show frame-relay multilink

Bundle:MFR0, State = up, class = A, fragmentation disabled
 BID = MFR0
 Bundle links :
 Serial2/1:3, HW state :up, Protocol state :Idle, LID :Serial2/1:3
 Serial2/1:2, HW state :up, Protocol state :Idle, LID :Serial2/1:2
 Serial2/1:1, HW state :up, Protocol state :Idle, LID :Serial2/1:1
```

The following is sample output from the **show frame-relay multilink** command when a Frame Relay bundle is configured as bandwidth class C (threshold) (see Table 36 for descriptions of the fields):

```
Router# show frame-relay multilink

Bundle: MFR0, state down, class C (threshold 2), no fragmentation
 ID: bundle
 Serial5/1, state up/up, ID: bundle1
 Serial5/3, state up/add-sent, ID: bundle3
```

Bundle Link: Example

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair (see Table 36 for descriptions of the fields). The example displays information about the specified bundle link:

```
Router# show frame-relay multilink serial 3/2

 Bundle links :
 Serial3/2, HW state : down, Protocol state :Down_idle, LID :Serial3/2
 Bundle interface = MFR0,  BID = MFR0
```

Detailed Bundle Links: Examples

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair and **detailed** keyword (see Table 36 for descriptions of the fields). The example shows a bundle link in the “idle” state:

```
Router# show frame-relay multilink serial 3 detailed

 Bundle links:

  Serial3, HW state = up, link state = Idle, LID = Serial3
  Bundle interface = MFR0,  BID = MFR0
    Cause code = none, Ack timer = 4, Hello timer = 10,
    Max retry count = 2, Current count = 0,
    Peer LID = Serial5/3, RTT = 0 ms
    Statistics:
    Add_link sent = 0, Add_link rcv'd = 10,
    Add_link ack sent = 0, Add_link ack rcv'd = 0,
    Add_link rej sent = 10, Add_link rej rcv'd = 0,
    Remove_link sent = 0, Remove_link rcv'd = 0,
    Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
    Hello sent = 0, Hello rcv'd = 0,
    Hello_ack sent = 0, Hello_ack rcv'd = 0,
    outgoing pak dropped = 0, incoming pak dropped = 0
```

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial** *number* keyword and argument pair and **detailed** keyword (see Table 36 for descriptions of the fields). The example shows a bundle link in the "up" state:

```
Router# show frame-relay multilink serial 3 detailed

 Bundle links:

  Serial3, HW state = up, link state = Up, LID = Serial3
  Bundle interface = MFR0,  BID = MFR0
    Cause code = none, Ack timer = 4, Hello timer = 10,
    Max retry count = 2, Current count = 0,
    Peer LID = Serial5/3, RTT = 4 ms
    Statistics:
    Add_link sent = 1, Add_link rcv'd = 20,
    Add_link ack sent = 1, Add_link ack rcv'd = 1,
    Add_link rej sent = 19, Add_link rej rcv'd = 0,
    Remove_link sent = 0, Remove_link rcv'd = 0,
    Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
    Hello sent = 0, Hello rcv'd = 1,
    Hello_ack sent = 1, Hello_ack rcv'd = 0,
    outgoing pak dropped = 0, incoming pak dropped = 0
```

Table 36 describes significant fields shown in the displays.

Table 36 show frame-relay multilink Field Descriptions

Field	Description
Bundle	Bundle interface.
State	Operational state of the bundle interface.
class	The bandwidth class criterion used to activate or deactivate a Frame Relay bundle. • Class A (single link)—The bundle activates when any bundle link is up and deactivates when all bundle links are down (default). • Class B (all links)—The bundle activates when all bundle links are up and deactivates when any bundle link is down. • Class C (threshold)—The bundle activates when the minimum configured number of bundle links (the threshold) is up and deactivates when the minimum number of configured bundle links fails to meet the threshold.
BID	Bundle identification.
Bundle links	Bundle links for which information is displayed.
HW state	Operational state of the physical link.
Protocol state	Operational state of the bundle link line protocol.
link state	Operational state of the bundle link.
LID	Bundle link identification.
Bundle interface	Bundle interface with which the bundle link is associated.

Table 36 show frame-relay multilink Field Descriptions (continued)

Field	Description
Cause code	Can be one of the following values: • ack timer expiry—Add link synchronization process is exhausted. • bundle link idle—Peer's bundle link is idle. This usually occurs when the peer's bundle interface is shut down. • inconsistent bundle—Peer already has this bundle associated with another bundle. • loopback detected—Local bundle link's physical line is looped back. • none—ADD_LINK and ADD_LINK_ACK messages were properly exchanged, and no cause code was recorded. • other—Indicates one of the following: a link identifier (LID) mismatch, an ID from the peer that is too long, or a failure to allocate ID memory. • unexpected Add_link—ADD_LINK message is received when the bundle link is already in the "up" state. This code might appear when the line protocol is being set up, but will disappear once the connection is stabilized.
Ack timer	Number of seconds for which the bundle link waits for a hello acknowledgment before resending a hello message or resending an ADD_LINK message used for initial synchronization.
Hello timer	Interval at which a bundle link sends out hello messages.
Max retry count	Maximum number of times that a bundle link will resend a hello message before receiving an acknowledgment or resending an ADD_LINK message.
Current count	Number of retries that have been attempted.
Peer LID	Bundle link identification name of the peer end of the link.
RTT	Round-trip time (in milliseconds) as measured by using the Timestamp Information Element in the HELLO and HELLO_ACK messages.
Statistics	Displays statistics for each bundle link.
Add_link sent	Number of Add_link messages sent. Add_link messages notify the peer endpoint that the local endpoint is ready to process frames.
Add_link rcv'd	Number of Add_link messages received.
Add_link ack sent	Number of Add_link acknowledgments sent. Add_link acknowledgments notify the peer endpoint that an Add_link message was received.
Add_link ack rcv'd	Number of Add_link acknowledgments received.
Add_link rej sent	Number of Add_link_reject messages sent.
Add_link rej rcv'd	Number of Add_link_reject messages received.

Table 36 show frame-relay multilink Field Descriptions (continued)

Field	Description
Remove_link sent	Number of Remove_link messages sent. Remove_link messages notify the peer that on the local end a bundle link is being removed from the bundle.
Remove_link rcv'd	Number of Remove_link messages received.
Remove_link_ack sent	Number of Remove_link acknowledgments sent. Remove_link acknowledgments notify the peer that a Remove_link message has been received.
Remove_link_ack rcv'd	Number of Remove_link acknowledgments received.
Hello sent	Number of hello messages sent. Hello messages notify the peer endpoint that the local endpoint remains in the "up" state.
Hello rcv'd	Number of hello messages received.
Hello_ack sent	Number of hello acknowledgments sent. Hello acknowledgments notify the peer that hello messages have been received.
Hello_ack rcv'd	Number of hello acknowledgments received.
outgoing pak dropped	Number of outgoing packets dropped.
incoming pak dropped	Number of incoming packets dropped.

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.

show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the **show frame-relay pvc** command in privileged EXEC mode.

show frame-relay pvc [[**interface** *interface*] [*dlci*] [**64-bit**] | **summary** [**all**]]

Syntax Description

interface	(Optional) Specific interface for which PVC information will be displayed.
interface	(Optional) Interface number containing the data-link connection identifiers (DLCIs) for which you wish to display PVC information.
dlci	(Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified.
64-bit	(Optional) Displays 64-bit counter statistics.
summary	(Optional) Displays a summary of all PVCs on the system.
all	(Optional) Displays a summary of all PVCs on each interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	This command was modified to display statistics about virtual access interfaces used for PPP connections over Frame Relay.
12.0(3)XG	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(4)T	This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC.
12.0(5)T	This command was modified to include information on the special voice queue that is created using the **queue** keyword of the **frame-relay voice bandwidth** command.
12.1(2)T	This command was modified to display the following information: • Details about the policy map attached to a specific PVC. • The priority configured for PVCs within Frame Relay PVC interface priority queueing. • Details about Frame Relay traffic shaping and policing on switched PVCs.
12.0(12)S	This command was modified to display reasons for packet drops and complete status information for switched NNI PVCs.
12.1(5)T	This command was modified to display the following information: • The number of packets in the post-hardware-compression queue. • The reasons for packet drops and complete status information for switched network-to-network PVCs.

Release	Modification
12.0(17)S	This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy.
12.2 T	This command was modified to show that when payload compression is configured for a PVC, the throughput rate reported by the PVC is equal to the rate reported by the interface.
12.2(4)T	The **64-bit** keyword was added.
12.2(11)T	This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy.
12.2(13)T	This command was modified to support display of Frame Relay PVC bundle information.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive fragmentation information.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC, and the **summary** and **all** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB, and support was added for hierarchical queueing framework (HQF).
12.4(9)T	The **summary** and **all** keywords were added, and support was added for hierarchical queueing framework (HQF).
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 monitor the PPP link control protocol (LCP) state as being open with an up state or closed with a down state.

When “vofr” or “vofr cisco” has been configured on the PVC, and a voice bandwidth has been allocated to the class associated with this PVC, configured voice bandwidth and used voice bandwidth are also displayed.

Statistics Reporting

To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.

To obtain statistics about a PVC that include policy-map configuration or the priority configured for that PVC, use this command with the *dlci* argument.

To display a summary of all PVCs on the system, use the **show frame-relay pvc** command with the **summary** keyword. To display a summary of all PVCs per interface, use the **summary all** keywords.

Per-VC counters are not incremented at all when either autonomous or silicon switching engine (SSE) switching is configured; therefore, PVC values will be inaccurate if either switching method is used.

You can change the period of time over which a set of data is used for computing load statistics. If you decrease the load interval, the average statistics are computed over a shorter period of time and are more responsive to bursts of traffic. To change the length of time for which a set of data is used to compute load statistics for a PVC, use the **load-interval** command in Frame-Relay DLCI configuration mode.

Traffic Shaping

Congestion control mechanisms are currently not supported on terminated PVCs nor on PVCs over ISDN. Where congestion control mechanisms are supported, the switch passes forward explicit congestion notification (FECN) bits, backward explicit congestion notification (BECN) bits, and discard eligible (DE) bits unchanged from entry points to exit points in the network.

Examples

The various displays in this section show sample output for a variety of PVCs. Some of the PVCs carry data only; some carry a combination of voice and data. This section contains the following examples:

Summary of Frame Relay PVCs: Example

The following example shows sample output of the **show frame-relay pvc** command with the **summary** keyword. The **summary** keyword displays all PVCs on the system.

```
Router# show frame-relay pvc summary

Frame-Relay VC Summary

              Active     Inactive      Deleted       Static
  Local          0           12            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
```

The following example shows sample output for the **show frame-relay pvc** command with the **summary** and **all** keywords. The **summary** and **all** keywords display all PVCs per interface.

```
Router# show frame-relay pvc summary all

VC Summary for interface Serial3/0 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          0            7            0            0
```

```
  Switched       0            0            0            0
  Unused         0            0            0            0

VC Summary for interface Serial3/1 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          0            5            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
```

Frame Relay Generic Configuration: Example

The following sample output shows a generic Frame Relay configuration on DLCI 100:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial4/0/1:0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE (EEK UP), INTERFACE = Serial4/0/1:0.1

  input pkts 4360          output pkts 4361         in bytes 146364
  out bytes 130252         dropped pkts 3735        in pkts dropped 0
  out pkts dropped 3735             out bytes dropped 1919790
  late-dropped out pkts 3735        late-dropped out bytes 1919790
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 337       out bcast bytes 102084
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 05:34:06, last time pvc status changed 05:33:38
```

Frame Relay Voice-Adaptive Fragmentation: Example

The following sample output indicates that Frame Relay voice-adaptive fragmentation is active on DLCI 202 and there are 29 seconds left on the deactivation timer. If no voice packets are detected in the next 29 seconds, Frame Relay voice-adaptive fragmentation will become inactive.

```
Router# show frame-relay pvc 202

PVC Statistics for interface Serial3/1 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial3/1.2

  input pkts 0             output pkts 479          in bytes 0
  out bytes 51226          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 5000 bits/sec, 5 packets/sec
  pvc create time 00:23:36, last time pvc status changed 00:23:31
  fragment type end-to-end fragment size 80 adaptive active, time left 29 secs
```

Frame Relay PVC Bundle: Example

The following sample output indicates that PVC 202 is a member of VC bundle MAIN-1-static:

```
Router# show frame-relay pvc 202

PVC Statistics for interface Serial1/4 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial1/4

  input pkts 0             output pkts 45           in bytes 0
```

```
  out bytes 45000          dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 2000 bits/sec, 2 packets/sec
  pvc create time 00:01:25, last time pvc status changed 00:01:11
  VC-Bundle MAIN-1-static
```

Frame Relay 64-Bit Counter: Example

The following sample output displays the Frame Relay 64-bit counters:

```
Router# show frame-relay pvc 35 64-bit

DLCI = 35, INTERFACE = Serial0/0
  input pkts 0                       output pkts 0
  in bytes 0                         out bytes 0
```

Frame Relay Fragmentation and Hardware Compression: Example

The following is sample output for the **show frame-relay pvc** command for a PVC configured with Cisco-proprietary fragmentation and hardware compression:

```
Router# show frame-relay pvc 110

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0/0

  input pkts 409           output pkts 409          in bytes 3752
  out bytes 4560           dropped pkts 1           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 3d00h, last time pvc status changed 2d22h
  Service type VoFR-cisco
   Voice Queueing Stats: 0/100/0 (size/max/dropped)
  Post h/w compression queue: 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
   64          16           2
  Output queue size 0/max total 600/drops 0
  configured voice bandwidth 16000, used voice bandwidth 0
  fragment type VoFR-cisco         fragment size 100
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 32000     byte increment 80    BECN response no
  frags 428       bytes 4810      frags delayed 24        bytes delayed 770
  shaping inactive
  traffic shaping drops 0
  ip rtp priority parameters 16000 32000 20000
```

Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command for a switched Frame Relay PVC. This output displays detailed information about Network-to-Network Interface (NNI) status and why packets were dropped from switched PVCs.

```
Router# show frame-relay pvc

 PVC Statistics for interface Serial2/2 (Frame Relay NNI)

 DLCI = 16, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial2/2
 LOCAL PVC STATUS = INACTIVE, NNI PVC STATUS = INACTIVE
```

```
  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  switched pkts0
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 00:00:07, last time pvc status changed 00:00:07
```

Frame Relay Congestion Management on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay congestion management is configured:

```
Router# show frame-relay pvc 200

PVC Statistics for interface Serial3/0 (Frame Relay DTE)

DLCI = 200, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial3/0

  input pkts 341           output pkts 390          in bytes 341000
  out bytes 390000         dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 390
  out bcast pkts 0          out bcast bytes 0            Num Pkts Switched 341

  pvc create time 00:10:35, last time pvc status changed 00:10:06
  Congestion DE threshold 50
  shaping active
  cir 56000     bc 7000      be 0         byte limit 875    interval 125
  mincir 28000     byte increment 875   BECN response no
  pkts 346       bytes 346000    pkts delayed 339       bytes delayed 339000
  traffic shaping drops 0
  Queueing strategy:fifo
  Output queue 48/100, 0 drop, 339 dequeued
```

Frame Relay Policing on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay policing is configured:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial1/0 (Frame Relay DCE)

DLCI = 100, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial1/0

  input pkts 1260          output pkts 0            in bytes 1260000
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0            Num Pkts Switched 1260

  pvc create time 00:03:57, last time pvc status changed 00:03:19
  policing enabled, 180 pkts marked DE
  policing Bc  6000        policing Be  6000        policing Tc  125 (msec)
  in Bc pkts   1080        in Be pkts   180         in xs pkts   0
  in Bc bytes  1080000     in Be bytes  180000      in xs bytes  0
```

Frame Relay PVC Priority Queueing: Example

The following is sample output for a PVC that has been assigned high priority:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 00:00:59, last time pvc status changed 00:00:33
  priority high
```

Low Latency Queueing for Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC shaped to a 64000 bps committed information rate (CIR) with fragmentation. A policy map is attached to the PVC and is configured with a priority class for voice, two data classes for IP precedence traffic, and a default class for best-effort traffic. Weighted Random Early Detection (WRED) is used as the drop policy on one of the data classes.

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial1/0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial1/0.1

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  pvc create time 00:00:42, last time pvc status changed 00:00:42
  service policy mypolicy
 Class voice
  Weighted Fair Queueing
      Strict Priority
      Output Queue: Conversation 72
        Bandwidth 16 (kbps) Packets Matched 0
        (pkts discards/bytes discards) 0/0
 Class immediate-data
  Weighted Fair Queueing
      Output Queue: Conversation 73
        Bandwidth 60 (%) Packets Matched 0
        (pkts discards/bytes discards/tail drops) 0/0/0
        mean queue depth: 0
        drops: class  random   tail     min-th   max-th   mark-prob
               0      0        0        64       128      1/10
               1      0        0        71       128      1/10
               2      0        0        78       128      1/10
               3      0        0        85       128      1/10
               4      0        0        92       128      1/10
               5      0        0        99       128      1/10
               6      0        0        106      128      1/10
               7      0        0        113      128      1/10
               rsvp   0        0        120      128      1/10
 Class priority-data
  Weighted Fair Queueing
      Output Queue: Conversation 74
```

```
       Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
       (pkts discards/bytes discards/tail drops) 0/0/0
 Class class-default
  Weighted Fair Queueing
      Flow Based Fair Queueing
      Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
  Output queue size 0/max total 600/drops 0
  fragment type end-to-end         fragment size 50
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 64000     byte increment 80    BECN response no
  frags 0         bytes 0         frags delayed 0         bytes delayed 0
  shaping inactive
  traffic shaping drops 0
```

PPP over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command that shows the PVC statistics for serial interface 5 (slot 1 and DLCI 55 are up) during a PPP session over Frame Relay:

```
Router# show frame-relay pvc 55

PVC Statistics for interface Serial5/1 (Frame Relay DTE)
DLCI = 55, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial5/1.1
     input pkts 9             output pkts 16           in bytes 154
     out bytes 338            dropped pkts 6           in FECN pkts 0
     in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
     in DE pkts 0             out DE pkts 0
     out bcast pkts 0         out bcast bytes 0
     pvc create time 00:35:11, last time pvc status changed 00:00:22
     Bound to Virtual-Access1 (up, cloned from Virtual-Template5)
```

Voice over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying Voice over Frame Relay (VoFR) traffic configured via the **vofr cisco** command. The **frame-relay voice bandwidth** command has been configured on the class associated with this PVC, as has fragmentation. The fragmentation type employed is proprietary to Cisco.

A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```
interface serial 0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 108
  vofr cisco
  class vofr-class
map-class frame-relay vofr-class
 frame-relay fragment 100
 frame-relay fair-queue
 frame-relay cir 64000
 frame-relay voice bandwidth 25000

Router# show frame-relay pvc 108

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 108, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 1260          output pkts 1271         in bytes 95671
  out bytes 98604          dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 1271       out bcast bytes 98604
  pvc create time 09:43:17, last time pvc status changed 09:43:17
  Service type VoFR-cisco
```

```
  configured voice bandwidth 25000, used voice bandwidth 0
  voice reserved queues 24, 25
  fragment type VoFR-cisco         fragment size 100
  cir 64000     bc 64000     be 0         limit 1000   interval 125
  mincir 32000     byte increment 1000  BECN response no
  pkts 2592      bytes 205140    pkts delayed 1296      bytes delayed 102570
  shaping inactive
  shaping drops 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
    64          16           2
  Output queue size 0/max total 600/drops 0
```

FRF.12 Fragmentation: Example

The following is sample output from the **show frame-relay pvc** command for an application employing pure FRF.12 fragmentation. A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```
interface serial 0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 110
  class frag
map-class frame-relay frag
 frame-relay fragment 100
 frame-relay fair-queue
 frame-relay cir 64000

Router# show frame-relay pvc 110

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 0             output pkts 243          in bytes 0
  out bytes 7290           dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 243        out bcast bytes 7290
  pvc create time 04:03:17, last time pvc status changed 04:03:18
  fragment type end-to-end         fragment size 100
  cir 64000     bc 64000     be 0         limit 1000   interval 125
  mincir 32000     byte increment 1000  BECN response no
  pkts 486       bytes 14580     pkts delayed 243       bytes delayed 7290
  shaping inactive
  shaping drops 0
  Current fair queue configuration:
   Discard     Dynamic      Reserved
   threshold   queue count  queue count
   64          16           2
  Output queue size 0/max total 600/drops 0
```

Note that when voice is not configured, voice bandwidth output is not displayed.

Multipoint Subinterfaces Transporting Data: Example

The following is sample output from the **show frame-relay pvc** command for multipoint subinterfaces carrying data only. The output displays both the subinterface number and the DLCI. This display is the same whether the PVC is configured for static or dynamic addressing. Note that neither fragmentation nor voice is configured on this PVC.

```
Router# show frame-relay pvc

DLCI = 300, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.103
input pkts 10  output pkts 7  in bytes 6222
out bytes 6034  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:13:11  last time pvc status changed 0:11:46
DLCI = 400, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.104
input pkts 20  output pkts 8  in bytes 5624
out bytes 5222  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:03:57  last time pvc status changed 0:03:48
```

PVC Shaping When HQF is Enabled: Example

The following is sample output from the **show frame-relay pvc** command for a PVC when HQF is enabled:

```
Router# show frame-relay pvc 16

PVC Statistics for interface Serial4/1 (Frame Relay DTE)

DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial4/1

  input pkts 1             output pkts 1            in bytes 34
  out bytes 34             dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 1         out bcast bytes 34
  pvc create time 00:09:07, last time pvc status changed 00:09:07
  shaping inactive
```

PVC Transporting Voice and Data: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying voice and data traffic, with a special queue specifically for voice traffic created using the **frame-relay voice bandwidth** command **queue** keyword:

```
Router# show frame-relay pvc interface serial 1 45

 PVC Statistics for interface Serial1 (Frame Relay DTE)

 DLCI = 45, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial1

   input pkts 85            output pkts 289          in bytes 1730
   out bytes 6580           dropped pkts 11          in FECN pkts 0
   in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
   in DE pkts 0             out DE pkts 0
   out bcast pkts 0          out bcast bytes 0
   pvc create time 00:02:09, last time pvc status changed 00:02:09
   Service type VoFR
   configured voice bandwidth 25000, used voice bandwidth 22000
   fragment type VoFR         fragment size 100
   cir 20000     bc   1000      be 0         limit 125    interval 50
   mincir 20000     byte increment 125   BECN response no
   fragments 290       bytes 6613      fragments delayed 1         bytes delayed 33
   shaping inactive
   traffic shaping drops 0
    Voice Queueing Stats: 0/100/0 (size/max/dropped)
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Current fair queue configuration:
 Discard     Dynamic      Reserved
 threshold   queue count  queue count
 64          16           2
Output queue size 0/max total 600/drops 0
```

Table 37 describes the significant fields shown in the displays.

Table 37 show frame-relay pvc Field Descriptions

Field	Description
DLCI	One of the DLCI numbers for the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.
PVC STATUS	Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE	Specific subinterface associated with this DLCI.
LOCAL PVC STATUS[1]	Status of PVC configured locally on the NNI interface.
NNI PVC STATUS[1]	Status of PVC learned over the NNI link.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.
in bytes	Number of bytes received on this PVC.
out bytes	Number of bytes sent on this PVC.
dropped pkts	Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
in pkts dropped	Number of incoming packets dropped. Incoming packets may be dropped for a number of reasons, including the following: • Inactive PVC • Policing • Packets received above DE discard level • Dropped fragments • Memory allocation failures • Configuration problems
out pkts dropped	Number of outgoing packets dropped, including shaping drops and late drops.
out bytes dropped	Number of outgoing bytes dropped.
late-dropped out pkts	Number of outgoing packets dropped because of QoS policy (such as with VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero.
late-dropped out bytes	Number of outgoing bytes dropped because of QoS policy (such with as VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero.
in FECN pkts	Number of packets received with the FECN bit set.
in BECN pkts	Number of packets received with the BECN bit set.

Table 37 show frame-relay pvc Field Descriptions (continued)

Field	Description
out FECN pkts	Number of packets sent with the FECN bit set.
out BECN pkts	Number of packets sent with the BECN bit set.
in DE pkts	Number of DE packets received.
out DE pkts	Number of DE packets sent.
out bcast pkts	Number of output broadcast packets.
out bcast bytes	Number of output broadcast bytes.
switched pkts	Number of switched packets.
no out intf[2]	Number of packets dropped because there is no output interface.
out intf down[2]	Number of packets dropped because the output interface is down.
no out PVC[2]	Number of packets dropped because the outgoing PVC is not configured.
in PVC down[2]	Number of packets dropped because the incoming PVC is inactive.
out PVC down[2]	Number of packets dropped because the outgoing PVC is inactive.
pkt too big[2]	Number of packets dropped because the packet size is greater than media MTU[3].
shaping Q full[2]	Number of packets dropped because the Frame Relay traffic-shaping queue is full.
pkt above DE[2]	Number of packets dropped because they are above the DE level when Frame Relay congestion management is enabled.
policing drop[2]	Number of packets dropped because of Frame Relay traffic policing.
pvc create time	Time at which the PVC was created.
last time pvc status changed	Time at which the PVC changed status.
VC-Bundle	PVC bundle of which the PVC is a member.
priority	Priority assigned to the PVC.
pkts marked DE	Number of packets marked DE because they exceeded the Bc.
policing Bc	Committed burst size.
policing Be	Excess burst size.
policing Tc	Measurement interval for counting Bc and Be.
in Bc pkts	Number of packets received within the committed burst.
in Be pkts	Number of packets received within the excess burst.
in xs pkts	Number of packets dropped because they exceeded the combined burst.
in Bc bytes	Number of bytes received within the committed burst.
in Be bytes	Number of bytes received within the excess burst.
in xs bytes	Number of bytes dropped because they exceeded the combined burst.
Congestion DE threshold	PVC queue percentage at which packets with the DE bit are dropped.
Congestion ECN threshold	PVC queue percentage at which packets are set with the BECN and FECN bits.

Table 37 show frame-relay pvc Field Descriptions (continued)

Field	Description
Service type	Type of service performed by this PVC. Can be VoFR or VoFR-cisco.
Post h/w compression queue	Number of packets in the post-hardware-compression queue when hardware compression and Frame Relay fragmentation are configured.
configured voice bandwidth	Amount of bandwidth in bits per second (bps) reserved for voice traffic on this PVC.
used voice bandwidth	Amount of bandwidth in bps currently being used for voice traffic.
service policy	Name of the output service policy applied to the VC.
Class	Class of traffic being displayed. Output is displayed for each configured class in the policy.
Output Queue	The WFQ[4] conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth in kbps or percentage configured for this class.
Packets Matched	Number of packets that matched this class.
Max Threshold	Maximum queue size for this class when WRED is not used.
pkts discards	Number of packets discarded for this class.
bytes discards	Number of bytes discarded for this class.
tail drops	Number of packets discarded for this class because the queue was full.
mean queue depth	Average queue depth, based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
drops:	WRED parameters.
class	IP precedence value.
random	Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
tail	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
min-th	Minimum WRED threshold in number of packets.
max-th	Maximum WRED threshold in number of packets.
mark-prob	Fraction of packets dropped when the average queue depth is at the maximum threshold.
Maximum Number of Hashed Queues	(Applies to class default only) Number of queues available for unclassified flows.
fragment type	Type of fragmentation configured for this PVC. Possible types are as follows: • end-to-end—Fragmented packets contain the standard FRF.12 header • VoFR—Fragmented packets contain the FRF.11 Annex C header • VoFR-cisco—Fragmented packets contain the Cisco proprietary header
fragment size	Size of the fragment payload in bytes.

Table 37 show frame-relay pvc Field Descriptions (continued)

Field	Description
adaptive active/inactive	Indicates whether Frame Relay voice-adaptive fragmentation is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive fragmentation deactivation timer. When this timer expires, Frame Relay fragmentation turns off.
cir	Current CIR in bps.
bc	Current committed burst (Bc) size, in bits.
be	Current excess burst (Be) size, in bits.
limit	Maximum number of bytes sent per internal interval (excess plus sustained).
interval	Interval being used internally (may be smaller than the interval derived from Bc/CIR; this happens when the router determines that traffic flow will be more stable with a smaller configured interval).
mincir	Minimum CIR for the PVC.
byte increment	Number of bytes that will be sustained per internal interval.
BECN response	Indication that Frame Relay has BECN adaptation configured.
pkts	Number of packets associated with this PVC that have gone through the traffic-shaping system.
frags	Total number of fragments (and unfragmented packets that are too small to be fragmented) shaped on this VC.
bytes	Number of bytes associated with this PVC that have gone through the traffic-shaping system.
pkts delayed	Number of packets associated with this PVC that have been delayed by the traffic-shaping system.
frags delayed	Number of fragments (and unfragmented packets that are too small to be fragmented) delayed in the shaping queue before being sent.
bytes delayed	Number of bytes associated with this PVC that have been delayed by the traffic-shaping system.
shaping	Indication that shaping will be active for all PVCs that are fragmenting data; otherwise, shaping will be active if the traffic being sent exceeds the CIR for this circuit.
shaping drops	Number of packets dropped by the traffic-shaping process.
Queueing strategy	Per-VC queueing strategy.
Output queue 48/100 0 drop 300 dequeued	State of the per-VC queue. • Number of packets enqueued/size of the queue • Number of packets dropped • Number of packets dequeued
Voice Queueing Stats	Statistics showing the size of packets, the maximum number of packets, and the number of packets dropped in the special voice queue created using the **frame-relay voice bandwidth** command **queue** keyword.

Table 37 show frame-relay pvc Field Descriptions (continued)

Field	Description
Discard threshold	Maximum number of packets that can be stored in each packet queue. Additional packets received after a queue is full will be discarded.
Dynamic queue count	Number of packet queues reserved for best-effort traffic.
Reserved queue count	Number of packet queues reserved for voice traffic.
Output queue size	Size in bytes of each output queue.
max total	Maximum number of packets of all types that can be queued in all queues.
drops	Number of frames dropped by all output queues.

1. The LOCAL PVC STATUS and NNI PVC STATUS fields are displayed only for PVCs configured on Frame Relay NNI interface types. These fields are not displayed if the PVC is configured on DCE or DTE interface types.
2. The detailed packet drop fields are displayed for switched Frame Relay PVCs only. These fields are not displayed for terminated PVCs.
3. MTU = maximum transmission unit.
4. WFQ = weighted fair queueing.

Related Commands

Command	Description
frame-relay accounting adjust	Enables byte count adjustment at the PVC level so that the number of bytes sent and received at the PVC corresponds to the actual number of bytes sent and received on the physical interface.
frame-relay interface-queue priority	Enables FR PIPQ on a Frame Relay interface and assigns priority to a PVC within a Frame Relay map class.
frame-relay pvc	Configures Frame Relay PVCs for FRF.8 Frame Relay-ATM Service Interworking.
service-policy	Attaches a policy map to an input interface or VC or an output interface or VC.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay map	Displays the current Frame Relay map entries and information about the connections
show frame-relay vc-bundle	Displays attributes and other information about a Frame Relay PVC bundle.

show frame-relay qos-autosense

To display the quality of service (QoS) values sensed from the switch, use the **show frame-relay qos-autosense** command in privileged EXEC mode.

show frame-relay qos-autosense [**interface** *number*]

Syntax Description

interface *number*	(Optional) Indicates the number of the physical interface for which you want to display QoS information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(3)T	This command was modified to display information about Enhanced Local Management Interface (ELMI) address registration.
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 is sample output from the **show frame-relay qos-autosense** command when ELMI and ELMI address registration are enabled.

```
Router# show frame-relay qos-autosense

ELMI information for interface Serial1
   IP Address used for Address Registration:9.2.7.9 My Ifindex:4
   ELMI AR status : Enabled.
   Connected to switch:hgw1 Platform:2611 Vendor:cisco
   Sw side ELMI AR status: Enabled
   IP Address used by switch for address registration :9.2.6.9 Ifindex:5
   ELMI AR status : Enabled.
               (Time elapsed since last update 00:00:40)
```

The following is sample output from the **show frame-relay qos-autosense** command when ELMI and traffic shaping are enabled:

```
Router# show frame-relay qos-autosense

ELMI information for interface Serial1
 Connected to switch:FRSM-4T1   Platform:AXIS   Vendor:cisco
              (Time elapsed since last update 00:00:30)

 DLCI = 100
 OUT:   CIR  64000       BC 50000        BE 25000        FMIF 4497
 IN:    CIR  32000       BC 25000        BE 12500        FMIF 4497
 Priority 0     (Time elapsed since last update 00:00:12)

 DLCI = 200
```

```
OUT:    CIR 128000       BC 50000        BE 5100         FMIF 4497
IN:     CIR Unknown      BC Unknown      BE Unknown      FMIF 4497
Priority 0     (Time elapsed since last update 00:00:13)
```

Table 38 describes the significant fields in the output display.

Table 38 show frame-relay qos-autosense Field Descriptions

Field	Description
IP Address used for Address Registration	Management IP address of the data terminal equipment (DTE) interface.
My ifIndex	ifIndex of the DTE interface on which ELMI is running.
ELMI AR status	Indicates whether ELMI is enabled or disabled on the interface.
Connected to switch	Name of neighboring switch.
Platform	Platform information about neighboring switch.
Vendor	Vendor information about neighboring switch.
Sw side ELMI AR status	Indicates whether ELMI is enabled or disabled on the neighboring switch.
IP Address used by switch for address registration	IP address of DCE. If ELMI is not supported or is disabled, this value will be 0.0.0.0.
ifIndex	ifIndex of DCE.
DLCI	Value that indicates which PVC statistics are being reported.
Out:	Values reporting settings configured for the outgoing Committed Information Rate, Burst Size, Excess Burst Size, and FMIF.
In:	Values reporting settings configured for the incoming Committed Information Rate, Burst Size, Excess Burst Size, and FMIF.
Priority	Value indicating priority level (currently not used).

Related Commands

Command	Description
frame-relay qos-autosense	Enables ELMI on the Cisco router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

show frame-relay route

To display all configured Frame Relay routes, along with their status, use the **show frame-relay route** command in privileged EXEC mode.

show frame-relay route

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 is sample output from the **show frame-relay route** command:

```
Router# show frame-relay route

    Input Intf      Input Dlci      Output Intf     Output Dlci  Status
    Serial1         100             Serial2         200          active
    Serial1         101             Serial2         201          active
    Serial1         102             Serial2         202          active
    Serial1         103             Serial3         203          inactive
    Serial2         200             Serial1         100          active
    Serial2         201             Serial1         101          active
    Serial2         202             Serial1         102          active
    Serial3         203             Serial1         103          inactive
```

Table 39 describes significant fields shown in the output.

Table 39 show frame-relay route Field Descriptions

Field	Description
Input Intf	Input interface and unit.
Input Dlci	Input DLCI number.
Output Intf	Output interface and unit.
Output Dlci	Output DLCI number.
Status	Status of the connection: active or inactive.

show frame-relay svc maplist

To display all the switched virtual circuits (SVCs) under a specified map list, use the **show frame-relay svc maplist** command in user EXEC or privileged EXEC mode.

show frame-relay svc maplist *name*

Syntax Description

name	Name of the map list.

Command Modes

User EXEC
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.

Examples

The following example shows, first, the configuration of the map list "fish" and, second, the corresponding output of the **show frame-relay svc maplist** command. The following lines show the configuration:

```
map-list fish local-addr X121 87654321 dest-addr X121 12345678
 ip 172.21.177.26 class fish ietf
 ipx 123.0000.0c07.d530 class fish ietf
!
map-class frame-relay fish
 frame-relay incir 192000
 frame-relay min-incir 19200
 frame-relay outcir 192000
 frame-relay min-outcir 19200
 frame-relay incbr(bytes) 15000
 frame-relay outcbr(bytes) 15000
```

The following lines show the output of the **show frame-relay svc maplist** command for the preceding configuration:

```
Router# show frame-relay svc maplist fish

Map List : fish
Local Address : 87654321           Type: X121
Destination Address: 12345678      Type: X121

Protocol : ip 172.21.177.26
Protocol : ipx 123.0000.0c07.d530
Encapsulation : IETF
Call Reference : 1             DLCI : 501

Configured Frame Mode Information Field Size :
Incoming : 1500         Outgoing : 1500
```

```
Frame Mode Information Field Size :
Incoming : 1500         Outgoing : 1500
Configured Committed Information Rate (CIR) :
Incoming : 192 * (10**3)                Outgoing : 192 * (10**3)
Committed Information Rate (CIR) :
Incoming : 192 * (10**3)                Outgoing : 192 * (10**3)
Configured Minimum Acceptable CIR :
Incoming : 192 * (10**2)                Outgoing : 192 * (10**2)
Minimum Acceptable CIR :
Incoming : 0 * (10**0)          Outgoing : 0 * (10**0)
Configured Committed Burst Rate (bytes) :
Incoming : 15000                Outgoing : 15000
Committed Burst Rate (bytes) :
Incoming : 15000                Outgoing : 15000
Configured Excess Burst Rate (bytes) :
Incoming : 16000                Outgoing : 1200
Excess Burst Rate (bytes) :
Incoming : 16000                Outgoing : 1200
```

Table 40 describes significant fields in the output.

Table 40 show frame-relay svc maplist Field Descriptions

Field	Description
Map List	Name of the configured map-list.
Local Address...Type	Configured source address type (E.164 or X.121) for the call.
Destination Address...Type	Configured destination address type (E.164 or X.121) for the call.
Protocol : ip ... Protocol: ipx ...	Destination protocol addresses configured for the map-list.
Encapsulation	Configured encapsulation type (CISCO or IETF) for the specified destination protocol address.
Call Reference	Call identifier.
DLCI: 501	Number assigned by the switch as the DLCI for the call.
Configured Frame Mode Information Field Size: Incoming: Outgoing: Frame Mode Information Field Size: Incoming: 1500 Outgoing: 1500	Lines that contrast the configured and actual frame mode information field size settings used for the calls.
Configured Committed Information Rate (CIR): Incoming: 192 * (10**3) Outgoing: 192 * (10**3) Committed Information Rate (CIR): Incoming: 192 * (10**3) Outgoing: 192 * (10**3)	Lines that contrast the configured and actual committed information rate (CIR) settings used for the calls.

Table 40 show frame-relay svc maplist Field Descriptions (continued)

Field	Description
Configured Minimum Acceptable CIR: Incoming: 192 * (10**2) Outgoing: 192 * (10**2) Minimum Acceptable CIR: Incoming: 0 * (10**0) Outgoing: 0 * (10**0)	Lines that contrast the configured and actual minimum acceptable CIR settings used for the calls.
Configured Committed Burst Rate (bytes): Incoming: 15000 Outgoing: 15000 Committed Burst Rate (bytes): Incoming: 15000 Outgoing: 15000	Lines that contrast the configured and actual committed burst rate (bytes) settings used for the calls.
Configured Excess Burst Rate (bytes): Incoming: 16000 Outgoing: 1200 Excess Burst Rate (bytes): Incoming: 16000 Outgoing: 1200	Lines that contrast the configured and actual excess burst rate (bytes) settings used for the calls.

Related Commands

Command	Description
class (map-list)	Associates a map class with a protocol-and-address combination.
frame-relay bc	Specifies the incoming or outgoing Bc for a Frame Relay VC.
frame-relay cir	Specifies the incoming or outgoing CIR for a Frame Relay VC.
frame-relay mincir	Specifies the minimum acceptable incoming or outgoing CIR for a Frame Relay VC.
map-class frame-relay	Specifies a map class to define QoS values for an SVC.
map-list	Specifies a map group and link 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.

show frame-relay traffic

To display the global Frame Relay statistics since the last reload, use the **show frame-relay traffic** command in privileged EXEC mode.

show frame-relay traffic

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 is sample output from the **show frame-relay traffic** command:

```
Router# show frame-relay traffic

Frame Relay statistics:
ARP requests sent 14, ARP replies sent 0
ARP request recvd 0, ARP replies recvd 10
```

show frame-relay vc-bundle

To display attributes and other information about a Frame Relay permanent virtual circuit (PVC) bundle, use the **show frame-relay vc-bundle** command in privileged EXEC mode.

show frame-relay vc-bundle *vc-bundle-name* [**detail**]

Syntax Description

vc-bundle-name	Name of this Frame Relay PVC bundle.
detail	(Optional) Displays output packet count information in addition to the other bundle member attributes for each PVC in the bundle specified by *vc-bundle-name*.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use this command to display packet service levels, bumping attributes, and other information about a specific Frame Relay PVC bundle. To view packet counts for each PVC in the bundle in addition to the other attributes, use the **detail** keyword.

Examples

Displaying General Information: Example

The following example shows the Frame Relay PVC bundle named “MP-4-dynamic” with PVC protection applied. Note that in this PVC bundle, data-link connection identifier (DLCI) 400 is configured to explicitly bump traffic to the PVC that handles DSCP level 40, which is DLCI 404. All the other DLCIs are configured for implicit bumping. In addition, all the DLCIs are configured to accept bumped traffic.

The asterisk (*) before PVC 4a indicates that this PVC was configured with the **precedence other** command, which means the PVC will handle all levels that are not explicitly configured on other PVCs.

In this example all PVCs are up so, the values in the “Active level” fields match the values in the “Config level” fields. If a PVC goes down and its traffic is bumped, the “Active level” field value for the PVC that went down is cleared. The “Active level” field values for the PVC that the traffic bumped to will be updated to include the levels of the PVC that went down.

The first three PVCs in the following example make up a protected group. All three of these PVCs must go down before the bundle will go down. The last two PVCs are protected PVCs: if either of these PVCs goes down, the bundle will go down.

```
Router# show frame-relay vc-bundle MP-4-dynamic

MP-4-dynamic on Serial1/4.1 - Status: UP Match-type: DSCP

Name    DLCI    Config. Active     Bumping    PG/     CIR     Status
                level   level      to/accept  PV      kbps
```

```
*4a     400     0-9     0-9         40/Yes      pg              up
4b      401     10-19   10-19       9/Yes       pg              up
4c      402     20-29   20-29       19/Yes      pg              up
4d      403     30-39   30-39       29/Yes      -               up
4e      404     40-49   40-49       39/Yes      -               up
4f      405     50-59   50-59       49/Yes      -               up
4g      406     60-62   60-62       59/Yes      pv              up
4h      407     63      63          62/Yes      pv              up

Packets sent out on vc-bundle MP-4-dynamic : 0:
Router#
```

Bumping: Example

The following example shows that although some DLCIs are down, the bumping rules and the remaining DLCIs keep the bundle up and running for all traffic types.

Note that DLCI 304 is handling the traffic being bumped from the three DLCIs that are down. The "Active level" field indicates the levels that the PVC is actually handling, not just which levels are configured.

```
Router# show frame-relay vc-bundle MP-3-static

MP-3-static on Serial1/4.1 - Status: UP Match-type: DSCP

Name    DLCI    Config. Active     Bumping    PG/     CIR     Status
                level   level      to/accept  PV      kbps
3a      300     0-9     0-9        -/Yes      -               up
3b      301     10-19   10-19      9/Yes      -               up
3c      302     20-29   20-29      19/Yes     -               up
3d      303     30-39              40/Yes     -               deleted
3e      304     40-49   30-59,63   39/Yes     -               up
3f      305     50-59              49/Yes     -               deleted
3g      306     60-62   60-62      59/No      -               up
3h      307     63                 62/Yes     -               deleted

Packets sent out on vc-bundle MP-3-static : 335
Router#
```

Traffic-Shaping: Example

The following example shows output for a PVC bundle configured with traffic shaping. The same rules of class inheritance apply to PVC-bundle members as to regular PVCs.

```
Router# show frame-relay vc-bundle 26k

26k on Serial1/4.1 - Status:UP  Match-type:PRECEDENCE

Name    DLCI  Config.         Active          Bumping     PG/ CIR   Status
              level           level           to/ accept  PV  kbps

        521   0,2,4           0,2,4           -/Yes       -   20    up
        522   1,3,5-6         1,3,5-6         0/Yes       -   26    up
        523   7               7               6/Yes       -   20    up

Packets sent out on vc-bundle 26k :0
Router#
```

Detail: Example

The following example shows the detail output of a PVC bundle. Note in this example that because all packet service levels are not handled, and because the PVCs are currently down, this bundle can never come up.

```
Router# show frame-relay vc-bundle x41 detail

x41 on Serial1/1 - Status: DOWN Match-type: DSCP

Name    DLCI    Config. Active     Bumping    PG/     CIR     Status
                level   level      to/accept  PV      kbps

        410     50-62              49/Yes     -               down
        411     30,32,34,36,3..    29/Yes     -               down

Packets sent out on vc-bundle x41 : 0

Active configuration and statistics for each member PVC
DLCI    Output pkts    Active level
410     0              50-62
411     0              30,32,34,36,38-40
Router#
```

Table 41 describes the significant fields shown in the **show frame-relay vc-bundle** displays.

Table 41 show frame-relay vc-bundle Field Descriptions

Field	Description
Status:	PVC bundle status. Possible values are UP, DOWN, and INITIAL (no PVCs associated with the bundle).
Name	The user-defined, alphanumeric name of the PVC.
DLCI	The ID number of the PVC bundle member.
Config. level	The packet service levels configured for the PVC.
Active level	The packet service levels actually handled by the PVC. This may include packet service levels for bumped traffic accepted by the PVC.
Bumping to/accept	The packet service level that the PVC will bump to if it goes down/whether or not the PVC will accept bumped traffic from another PVC.
PG/PV	Indicates whether the PVC is a member of a protected group or is an individually protected PVC. A dash in this field indicates that the PVC is not protected.
CIR kbps	Committed information rate for the PVC, in kilobits per second.
Status	Indicates whether the PVC is up, down, or deleted.
Output pkts	Number of packets sent out on the PVC.

Related Commands

Command	Description
show frame-relay map	Displays the current Frame Relay map entries and information about the connections.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.

show l2cac

To display dynamic Layer 2 Call Admission Control (L2CAC) information for an asynchronous transfer mode (ATM) interface, use the **show l2cac** command in user EXEC or privileged EXEC mode.

show l2cac atm *interface-number* {**aggregate-svc** | **vcd** *vcd-number*}

Syntax Description

atm	Specifies an ATM interface.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
aggregate-svc	Aggregates switched virtual circuits (SVCs).
vcd	Specifies the virtual circuit descriptor (VCD) about which the L2CAC information must be displaced.
vcd-number	VCD number. The range is from 1 to 65535.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show l2cac** command for aggregated SVCs on ATM interface 2/0:

```
Router# show l2cac atm2/0 aggregate-svc

*Jun 11 04:01:44.247: l2_cac_show_cmd. Begin
*Jun 11 04:01:44.247: l2_cac_show_cmd: l2 cac control block not found, with the vcd = 0
*Jun 11 04:01:44.247: l2_cac_show_cmd. End
```

The following is sample output from the **show l2cac** command for VCD 1 on ATM interface 2/0:

```
Router# show l2cac atm2/0 vcd 1

vcci number = 1.
*Jun 11 04:02:16.487: l2_cac_show_cmd. Begin
*Jun 11 04:02:16.487: l2_cac_show_cmd: l2 cac control block not found, with the vcd = 1
*Jun 11 04:02:16.487: l2_cac_show_cmd. End
```

Table 42 describes the significant fields shown in the displays.

Table 42 show l2cac Field Descriptions

Field	Description
Begin	Indicates the beginning of the output.
l2 cac control block not found, with the vcd = 0	Displays the status of the L2CAC and the VCD number.
End	Indicates the end of the output.
vcci number	Displays the Virtual Circuit Connection Identifier (VCCI) number.

Related Commands

Command	Description
codec aal2-profile atmf	Configures the ATMF profile for VoAAL2.

show l2tun

To display general information about Layer 2 tunnels and sessions, use the **show l2tun** command in privileged EXEC mode.

show l2tun

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

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

The **show l2tun** command displays general information about all active Layer 2 tunnels and sessions. Use the **show l2tun tunnel** command or the **show l2tun session** command to display more detailed information about Layer 2 tunnels or sessions.

Examples

The following example shows the display of information about all currently active Layer 2 tunnels and sessions:

```
Router# show l2tun

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
                                                          VPDN Group
45795 43092 PE1           est    10.1.1.1         0     1        generic

LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
42410      0          45795      123456789, Fa4/1/1   idle   00:00:24 1
```

Table 43 describes the significant fields shown in the display.

Table 43 show l2tun tunnel all Field Descriptions

Field	Description
Total tunnels	Total number of tunnels established on the router.
sessions	Total number of sessions established on the router.
LocID	Local ID of the tunnel.

Table 43 show l2tun tunnel all Field Descriptions (continued)

Field	Description
RemID	Remote ID of the tunnel.
Remote Name	Hostname of the remote tunnel endpoint.
State	State of the tunnel.
Remote Address	IP address of the remote tunnel endpoint.
Port	Port number used by the remote tunnel endpoint.
Sessions	Number of sessions established in the tunnel.
L2TPclass	Name of the L2TP class the tunnel parameters are derived from.
VPDN group	Name of the virtual private dial-up network (VPDN) group the tunnel belongs to.
LocID	Local ID of the session.
RemID	Remote ID of the session.
TunID	Tunnel ID of the tunnel the session is in.
Username, Intf/Vcid, Circuit	The sessions username, interface, virtual circuit identifier (VCID), and circuit.
Last Chg	Time since the last change in the tunnel state, in hh:mm:ss.
Uniq ID	The tunnel session ID.

Related Commands

Command	Description
clear l2tun tunnel counters	Clears L2TP control channel authentication counters.
show l2tun session	Displays the current state of Layer 2 sessions and displays protocol information about L2TP control channels.
show l2tun tunnel	Displays the current state of a Layer 2 tunnel and displays information about currently configured tunnels.

show l2tun counters tunnel l2tp

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

show l2tun counters tunnel l2tp [**all** | **authentication** | **id** *local-id*]

Syntax Description

all	(Optional) Displays control message statistics for all L2TP tunnels that have per-tunnel statistics enabled.
authentication	(Optional) Displays global information about L2TP control channel authentication attribute-value (AV) pairs.
id *local-id*	(Optional) Displays control message statistics for the L2TP tunnel with the specified local ID.

Command Default

Global control message statistics are always enabled.
Per-tunnel control message statistics are disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB, and EXP ACK and CiscoACK were added to the command output.

Usage Guidelines

Use the **show l2tun counters tunnel l2tp** command to display global L2TP control message statistics.

Use the **show l2tun counters tunnel l2tp authentication** command to display global L2TP authentication control message statistics.

The **show l2tun counters tunnel l2tp** command can display per-tunnel statistics, but per-tunnel statistics must first be enabled. Per-tunnel statistics are controlled on a tunnel by tunnel basis using the **monitor l2tun counters tunnel l2tp** command.

Use the **show l2tun counters tunnel l2tp id** *local-id* command to display per-tunnel statistics for a specific tunnel.

Use the **show l2tun counters tunnel l2tp all** command to display control message statistics for all tunnels that have per-tunnel statistics enabled.

Examples

The following example displays global L2TP control message counter information. In this example, the `Number of unknown control messages received:` displays only if the unknown message count is nonzero.

```
Router# show l2tun counters tunnel l2tp

Global L2TP tunnel control message statistics:
 Number of unknown control messages received: 10

                  XMIT       RE-XMIT         RCVD         DROP
              ==========   ==========   ==========   ==========
Total               32           25           22           15
ZLB                  0            0            0            0
SCCRQ                6           10            0            0
SCCRP                0            0            1            0
SCCCN                1            0            0            0
StopCCN              5            5            0            0
Hello                0            0            0            0
OCRQ                 0            0            0            0
OCRP                 0            0            0            0
OCCN                 0            0            0            0
ICRQ                 2            0            0            0
ICRP                 0            0            2            0
ICCN                 2            0            0            0
CDN                  0            0            0            0
WEN                  0            0            0            0
SLI                  2            0            4            0
EXP ACK              0            0            0            0
SRRQ                 0            0            0            0
SRRP                 0            0            0            0
CiscoACK             4            0            5            5
```

Table 44 describes the significant fields shown in the display.

Table 44 show l2tun counters tunnel l2tp Field Descriptions

Field	Description
XMIT	The number of control messages that have been sent.
RE-XMIT	The number of control messages that have been sent.
RCVD	The number of control messages that have been received.
DROP	The number of control messages that have been dropped.
ZLB	The number of Zero Length Body (ZLB) messages.
SCCRQ	The number of Start-Control-Connection-Request (SCCRQ) messages.
SCCRP	The number of Start-Control-Connection-Reply (SCCRP) messages.
SCCCN	The number of Start-Control-Connection-Connected (SCCCN) messages.
StopCCN	The number of Stop-Control-Connection-Notification (StopCCN) messages.
Hello	The number of hello messages.
OCRQ	The number of Outgoing-Call-Request (OCRQ) messages.
OCRP	The number of Outgoing-Call-Reply (OCRP) messages.
OCCN	The number of Outgoing-Call-Connected (OCCN) messages.
ICRQ	The number of Incoming-Call-Request (ICRQ) messages.
ICRP	The number of Incoming-Call-Reply (ICRP) messages.

Table 44 show l2tun counters tunnel l2tp Field Descriptions (continued)

Field	Description
ICCN	The number of Incoming-Call-Connected (ICCN) messages.
CDN	The number of Call-Disconnect-Notify (CDN) messages.
WEN	The number of WAN-Error-Notify (WEN) messages.
SLI	The number of Set-Link-Info (SLI) messages.
EXP ACK	The number of Explicit-Acknowledgment (ACK) messages.
SRRQ	The number of Service Relay Request Message (SRRQ) messages.
SRRP	The number of Service Relay Reply Message (SRRP) messages.
CiscoACK	The number of Cisco Explicit-Acknowledgment (ACK) messages.

The following example shows the display of all possible L2TP control channel authentication AV pair statistics. AV pair statistic fields are displayed only if they are nonzero. For the purposes of this example, all possible output fields are displayed in the sample output.

```
Router# show l2tun counters tunnel l2tp authentication

 L2TPv3 Tunnel Authentication Statistics:
   Nonce AVP Statistics:
     Ignored                                0
     Missing                                0
   All Digests Statistics:
     Unexpected                             0
     Unexpected ZLB                         0
   Primary Digest AVP Statistics:
     Validate fail                          0
     Hash invalid                           0
     Length invalid                         0
     Missing                                0
     Ignored                                0
     Passed                                 0
     Failed                                 0
   Secondary Digest AVP Statistics:
     Validate fail                          0
     Hash invalid                           0
     Length invalid                         0
     Missing                                0
     Ignored                                0
     Passed                                 0
     Failed                                 0
   Integrity Check Statistics:
     Validate fail                          0
     Length invalid                         0
     Passed                                 0
     Failed                                 0
   Local Secret Statistics:
     Missing                                0
   Challenge AVP Statistics:
     Generate response fail                 0
     Ignored                                0
   Challenge/Response AVP Statistics:
     Generate response fail                 0
     Missing                                0
     Ignored                                0
     Passed                                 0
     Failed                                 0
```

```
Overall Statistics:
  Passed                                0
  Skipped                               0
  Ignored                               0
  Failed                                0
```

Table 45 describes the significant fields shown in the display.

Table 45 show l2tun counters tunnel l2tp authentication Field Descriptions

Field	Description
Nonce AVP Statistics	Counters for the nonce AV pair.
Ignored	Number of AV pair messages that were ignored.
Missing	Number of AV pair messages that were missing.
All Digests Statistics	Statistics for all configured digest passwords.
Unexpected	Digest information was received but the router is not configured for it.
Unexpected ZLB	A ZLB message was received while control message authentication is enabled. ZLB messages are permitted only when control message authentication is disabled.
Primary Digest AVP Statistics	Statistics for AV pair messages exchanged using the primary L2TP Version 3 (L2TPv3) control message digest password.
Validate fail	Number of AV pair messages that failed to validate.
Hash invalid	Number of AV pair messages with an invalid hash.
Length invalid	Number of AV pair messages with an invalid length.
Passed	Number of AV pair messages successfully exchanged.
Failed	Number of AV pair messages that have failed to authenticate.
Secondary Digest AVP Statistics	Statistics for AV pair messages exchanged using the secondary L2TPv3 control message digest password.
Integrity Check Statistics	Statistics for AV pair messages exchanged when integrity checking is enabled.
Local Secret Statistics	Statistics for AV pair messages related to the local secret.
Challenge AVP Statistics	Statistics for AV pair messages related to Challenge Handshake Authentication Protocol (CHAP) style authentication challenges.
Generate response fail	Number of AV pair messages that did not generate a response.
Challenge/Response AVP Statistics	Statistics for AV pair messages exchanged when CHAP-style authentication is configured.
Overall Statistics	Summary of the statistics for all authentication AV pair messages.
Skipped	The number of AV pair messages that authentication was not performed on.

The following example displays L2TP control message statistics for all L2TP tunnels with per-tunnel statistics enabled:

```
Router# show l2tun counters tunnel l2tp all

Summary listing of per-tunnel statistics:

   LocID  RemID  Remote IP       Total     Total     Total     Total
                                 XMIT      RE-XMIT   RCVD      DROP
   15587  39984  10.0.1.1       40        0         40        0
   17981  42598  10.0.0.1       34        0         34        0
   22380  14031  10.0.0.0       38        0         38        0
   31567  56228  10.0.1.0       32        0         32        0
   38360  30275  10.1.1.1       30        0         30        0
   42759  1708   10.1.0.1       36        0         36        0

Number of tunnels with per-tunnel stats: 6
```

Table 46 describes the significant fields shown in the display.

Table 46 show l2tun counters tunnel l2tp all Field Descriptions

Field	Description
LocID	The local tunnel ID.
RemID	The remote tunnel ID.
Remote IP	The IP address of the remote peer.
Total XMIT	Total number of control messages sent.
Total RE-XMIT	Total number of control messages sent.
Total RCVD	Total number of control messages received.
Total Drop	Total number of control messages dropped.

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

```
Router# monitor l2tun counters tunnel l2tp id 38360 start
Router#
```

The following example displays L2TP control message statistics for the L2TP tunnel with the local ID 38360:

```
Router# show l2tun counters tunnel l2tp id 38360

L2TP tunnel control message statistics:
   Tunnel LocID: 38360  RemID: 30275
   Remote Address: 10.1.1.1

                  XMIT       RE-XMIT         RCVD         DROP
               ==========   ==========   ==========   ==========
Total                32           25           22           15
ZLB                   0            0            0            0
SCCRQ                 6           10            0            0
SCCRP                 0            0            1            0
SCCCN                 1            0            0            0
StopCCN               5            5            0            0
Hello                 0            0            0            0
OCRQ                  0            0            0            0
OCRP                  0            0            0            0
OCCN                  0            0            0            0
```

```
ICRQ                2           0           0           0
ICRP                0           0           2           0
ICCN                2           0           0           0
CDN                 0           0           0           0
WEN                 0           0           0           0
SLI                 2           0           4           0
EXP ACK             0           0           0           0
SRRQ                0           0           0           0
SRRP                0           0           0           0
CiscoACK            4           0           5           5
```

Related Commands

Command	Description
clear l2tun counters	Clears L2TP session counters.
clear l2tun counters tunnel l2tp	Clears global or per-tunnel control message statistics for L2TP tunnels.
monitor l2tun counters tunnel l2tp	Enables or disables the collection of per-tunnel control message statistics for L2TP tunnels.
show l2tun tunnel	Displays the current state of L2TP tunnels and information about configured tunnels.

show l2tun session

To display the current state of Layer 2 sessions and protocol information about Layer 2 Tunnel Protocol (L2TP) control channels, use the **show l2tun session** command in privileged EXEC mode.

show l2tun session [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets** [*filter*] | **sequence** [*filter*] | **state** [*filter*]]

Syntax Descriptions

l2tp	(Optional) Displays information about L2TP.
pptp	(Optional) Displays information about Point-to-Point Tunneling Protocol.
all	(Optional) Displays information about all current L2TP sessions on the router.
filter	(Optional) One of the filter parameters defined in Table 47.
brief	(Optional) Displays information about all current L2TP sessions, including the peer ID address and circuit status of the L2TP sessions.
hostname	(Optional) Specifies that the peer hostname will be displayed in the output.
circuit	(Optional) Displays information about all current L2TP sessions, including circuit status (up or down).
interworking	(Optional) Displays information about Layer 2 Virtual Private Network (L2VPN) interworking.
packets	(Optional) Displays information about the packet counters (in and out) associated with current L2TP sessions.
sequence	(Optional) Displays sequencing information about each L2TP session, including the number of out-of-order and returned packets.
state	(Optional) Displays information about all current L2TP sessions and their protocol state, including remote Virtual Connection Identifiers (VCIDs).

Command Modes

Privileged EXEC (#)

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.
12.0(31)S	The **hostname** keyword was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	This command was modified.The **pptp** and **tunnel** keywords were added.

Usage Guidelines

Use the **show l2tun session** command to display information about current L2TP sessions on the router.

Table 47 defines the filter parameters available to refine the output of the **show l2tun session** command.

Table 47 Filter Parameters for the show l2tun session Command

Syntax	Description
ip-addr *ip-address* [**vcid** *number*]	Filters the output to display information about only those L2TP sessions associated with the IP address of the peer router. The 32-bit VCID shared between the peer router and the local router at each end of the control channel can be optionally specified. • *ip-address*—IP address of the peer router. • *number*—VCID number.
vcid *number*	Filters the output to display information about only those L2TP sessions associated with the VCID shared between the peer router and the local router at each end of the control channel. • *number*—VCID number.
username *username*	Filters the output to display information for only those sessions associated with the specified username. • *username*—Username.
tunnel {**id** *local-tunnel local-session* | **remote-name** *remote-tunnel local-tunnel-name*}	Displays the sessions in a tunnel. • **id**—Tunnel ID for established tunnels. • *local-tunnel*—Local tunnel ID. • *local-session*—Local session ID. • **remote-name**—Remote tunel name. • *remote-tunnel*—Remote tunnel name. • *local-tunnel*—Local tunnel name.

Examples

The following example shows how to display detailed information about all current L2TP sessions:

```
Router# show l2tun session all

Session Information Total tunnels 0 sessions 1

Session id 42438 is down, tunnel id n/a
  Remote session id is 0, remote tunnel id n/a
Session Layer 2 circuit, type is Ethernet, name is FastEthernet4/1/1
  Session vcid is 123456789
  Circuit state is DOWN
    Local circuit state is DOWN
    Remote circuit state is DOWN
Call serial number is 1463700128
Remote tunnel name is PE1
  Internet address is 10.1.1.1
Local tunnel name is PE1
  Internet address is 10.1.1.2
IP protocol 115
  Session is L2TP signalled
  Session state is idle, time since change 00:00:26
    0 Packets sent, 0 received
    0 Bytes sent, 0 received
  Last clearing of "show vpdn" counters never
```

```
    Receive packets dropped:
      out-of-order:            0
      total:                   0
    Send packets dropped:
      exceeded session MTU:    0
      total:                   0
  DF bit off, ToS reflect disabled, ToS value 0, TTL value 255
  No session cookie information available
  UDP checksums are disabled
  L2-L2 switching enabled
  No FS cached header information available
  Sequencing is off
  Unique ID is 1
```

The following example shows how to display information only about the L2TP session set up on a peer router with an IP address of 192.0.2.0 and a VCID of 300:

```
Router# show l2tun session all ip-addr 192.0.2.0 vcid 300

L2TP Session
Session id 32518 is up, tunnel id n/a
Call serial number is 2074900020
Remote tunnel name is tun1
  Internet address is 192.0.2.0
Session is L2TP signalled
  Session state is established, time since change 03:06:39
    9932 Packets sent, 9932 received
    1171954 Bytes sent, 1171918 received
  Session vcid is 300
  Session Layer 2 circuit, type is Ethernet Vlan, name is FastEthernet0/1/0.3:3
  Circuit state is UP
    Remote session id is 18819, remote tunnel id n/a
  Set DF bit to 0
  Session cookie information:
    local cookie, size 4 bytes, value CF DC 5B F3
    remote cookie, size 4 bytes, value FE 33 56 C4
  SSS switching enabled
  Sequencing is on
    Ns 9932, Nr 10001, 0 out of order packets discarded
```

Table 48 describes the significant fields shown in the displays.

Table 48 show l2tun session Field Descriptions

Field	Description
Total tunnels	Total number of L2TP tunnels established on the router.
sessions	Number of L2TP sessions established on the router.
Session id	Session ID for established sessions.
is	Session state.
tunnel id	Tunnel ID for established tunnels.
Remote session id	Session ID for the remote session.
tunnel id	Tunnel ID for the remote tunnel.
Session Layer 2 circuit, type is, name is	Type and name of the interface used for the Layer 2 circuit.
Session vcid is	VCID of the session.

Table 48 show l2tun session Field Descriptions (continued)

Field	Description
Circuit state is	State of the Layer 2 circuit.
Local circuit state is	State of the local circuit.
Remote circuit state is	State of the remote circuit.
Call serial number is	Call serial number.
Remote tunnel name is	Name of the remote tunnel.
Internet address is	IP address of the remote tunnel.
Local tunnel name is	Name of the local tunnel.
Internet address is	IP address of the local tunnel.
IP protocol	The IP protocol used.
Session is	Signaling type for the session.
Session state is	Session state for the session.
time since change	Time since the session state last changed, in the format hh:mm:ss.
Packets sent, received	Number of packets sent and received since the session was established.
Bytes sent, received	Number of bytes sent and received since the session was established.
Last clearing of "show vpdn" counters	Time elapsed since the last clearing of the counters displayed with the **show vpdn** command. Time will be displayed in one of the following formats: • hh:mm:ss—Hours, minutes, and seconds. • dd:hh—Days and hours. • WwDd—Weeks and days, where W is the number of weeks and D is the number of days. • YyWw—Years and weeks, where Y is the number of years and W is the number of weeks. • never—The timer has not been started.
Receive packets dropped:	Number of received packets that were dropped since the session was established. • out-of-order—Total number of received packets that were dropped because they were out of order. • total—Total number of received packets that were dropped.
Send packets dropped:	Number of sent packets that were dropped since the session was established. • exceeded session MTU—Total number of sent packets that were dropped because the session maximum transmission unit (MTU) was exceeded. • total—Total number of sent packets that were dropped.
DF bit	Status of the Don't Fragment (DF) bit option. The DF bit can be on or off.
ToS reflect	Status of the type of service (ToS) reflect option. ToS reflection can be enabled or disabled.
ToS value	Value of the ToS byte in the L2TP header.
TTL value	Value of the time-to-live (TTL) byte in the L2TP header.

Table 48 show l2tun session Field Descriptions (continued)

Field	Description
local cookie	Size (in bytes) and value of the local cookie.
remote cookie	Size (in bytes) and value of the remote cookie.
UDP checksums are	Status of the User Datagram Protocol (UDP) checksum configuration.
switching	Status of switching.
No FS cached header information available	Fast Switching (FS) cached header information. If an FS header is configured, the encapsulation size and hexadecimal contents of the FS header will be displayed. The FS header is valid only for IP virtual private dialup network (VPDN) traffic from a tunnel server to a network access server (NAS).
Sequencing is	Status of sequencing. Sequencing can be on or off.
Ns	Sequence number for sending.
Nr	Sequence number for receiving.
Unique ID is	Global user ID correlator.

The following example shows how to display information about the circuit status of L2TP sessions on a router:

```
Router# show l2tun session circuit

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-address    Type Stat Username, Intf/
                                              Vcid, Circuit
32517      n/a         172.16.184.142  VLAN UP   100, Fa0/1/0.1:1
32519      n/a         172.16.184.142  VLAN UP   200, Fa0/1/0.2:2
32518      n/a         172.16.184.142  VLAN UP   300, Fa0/1/0.3:3
```

The following example shows how to display information about the circuit status of L2TP sessions and the hostnames of remote peers:

```
Router# show l2tun session circuit hostname

Session Information Total tunnels 3 sessions 3

LocID      TunID      Peer-hostname Type Stat Username, Intf/
                                              Vcid, Circuit
32517      n/a         <unknown>       VLAN UP   100, Fa0/1/0.1:1
32519      n/a         router32        VLAN UP   200, Fa0/1/0.2:2
32518      n/a         access3         VLAN UP   300, Fa0/1/0.3:3
```

Table 49 describes the significant fields shown in the displays.

Table 49 show l2tun session circuit Field Descriptions

Field	Description
LocID	Local session ID.
TunID	Tunnel ID.
Peer-address	IP address of the peer.
Peer-hostname	Hostname of the peer.
Type	Session type.

Table 49 show l2tun session circuit Field Descriptions (continued)

Field	Description
Stat	Session status.
Username, Intf/Vcid, Circuit	Username, interface name/VCID, and circuit number of the session.

Related Commands

Command	Description
show l2tun	Displays general information about Layer 2 tunnels and sessions.
show l2tun tunnel	Displays the current state of Layer 2 tunnels and information about configured tunnels.

show l2tun tunnel

To display the current state of Layer 2 Tunneling Protocol (L2TP) tunnels and information about configured tunnels, including local and remote hostnames, aggregate packet counts, and control channel information, use the **show l2tun tunnel** command in privileged EXEC mode.

show l2tun tunnel [**l2tp** | **pptp**] [**all** [*filter*] | **packets** [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport** [*filter*] | **authentication**]

Syntax Description

l2tp	(Optional) Displays information about L2TP.
pptp	(Optional) Displays information about Point-to-Point Tunneling Protocol.
all	(Optional) Displays information about all current L2TP sessions configured on the router.
filter	(Optional) One of the filter parameters defined in Table 50.
packets	(Optional) Displays aggregate packet counts for all negotiated L2TP sessions.
state	(Optional) Displays information about the current state of L2TP sessions, including the local and remote hostnames for each control channel.
summary	(Optional) Displays a summary of L2TP sessions on the router and their current state, including the number of virtual private dialup network (VPDN) sessions associated with each control channel.
transport	(Optional) Displays information about the L2TP control channels used in each session and the local and remote IP addresses at each end of the control channel.
authentication	(Optional) Displays global information about L2TP control channel authentication attribute-value pairs (AV pairs).

Command Modes

Privileged EXEC (#)

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.
12.0(30)S	This command was enhanced to display information about pseudowire control channel authentication passwords.
12.0(31)S	The **authentication** keyword was added and the output of the **show l2tun tunnel all** command was enhanced to display per-tunnel authentication failure counters.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	The **authentication** keyword was removed. The statistics previously displayed by the **show l2tun tunnel authentication** command are now displayed by the **show l2tun counters tunnel l2tp authentication** command.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

Use the **show l2tun tunnel** command to display information about configured L2TP sessions on the router.

Table 50 defines the filter parameters available to refine the output of the **show l2tun tunnel** command.

Table 50 Filter Parameters for the show l2tun tunnel Command

Syntax	Description
id *local-id*	Filters the output to display information for only the tunnel with the specified local ID. • *local-id*—The local tunnel ID number. Valid values range from 1 to 65535.
local-name *local-name remote-name*	Filters the output to display information for only the tunnel associated with the specified names. • *local-name*—The local tunnel name. • *remote-name*—The remote tunnel name.
remote-name *remote-name local-name*	Filters the output to display information for only the tunnel associated with the specified names. • *remote-name*—The remote tunnel name. • *local-name*—The local tunnel name.

Examples

The following example shows how to display detailed information about all L2TP tunnels:

```
Router# show l2tun tunnel all

Tunnel Information Total tunnels 1 sessions 1

Tunnel id 26515 is up, remote id is 41814, 1 active sessions
  Tunnel state is established, time since change 03:11:50
  Tunnel transport is IP (115)
  Remote tunnel name is tun1
    Internet Address 172.0.0.0, port 0
  Local tunnel name is Router
    Internet Address 172.0.0.1, port 0
  Tunnel domain is
  VPDN group for tunnel is
  L2TP class for tunnel is
  0 packets sent, 0 received
  0 bytes sent, 0 received
  Control Ns 11507, Nr 11506
  Local RWS 2048 (default), Remote RWS 800
  Tunnel PMTU checking disabled
```

```
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 1, max 1
Total resends 0, ZLB ACKs sent 11505
Total peer authentication failures 8
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
Sessions disconnected due to lack of resources 0
```

Table 51 describes the significant fields shown in the displays.

Table 51 show l2tun tunnel all Field Descriptions

Field	Description
Total tunnels	Total number of L2TP tunnels currently established on the router.
sessions	Number of L2TP sessions currently established on the router.
Tunnel id is up	Tunnel ID and tunnel status.
remote id is	Remote ID.
active sessions	Number of active sessions.
Tunnel state is	State of the tunnel.
time since change	Time since the tunnel state last changed, in the format hh:mm:ss.
Tunnel transport is	Tunnel transport protocol.
Remote tunnel name is	Name of the remote tunnel endpoint.
Internet Address	IP address of the remote tunnel endpoint.
port	Port number used by the remote tunnel endpoint.
Local tunnel name is	Name of the local tunnel endpoint.
Internet Address	IP address of the local tunnel endpoint.
port	Port number used by the local tunnel endpoint.
Tunnel domain is	Domain information for the tunnel.
VPDN group for tunnel is	Name of the VPDN group associated with the tunnel.
L2TP class for tunnel is	Name of the L2TP class associated with the tunnel.
packets sent, received	Number of packets sent and received since the tunnel was established.
bytes sent, received	Number of bytes sent and received since the tunnel was established.
Control Ns, Nr	Sequence number for control packets sent and received.
Local RWS	Local receiving window size, in packets.
Remote RWS	Remote receiving window size, in packets.
Tunnel PMTU checking	Status of the tunnel path maximum transmission unit (MTU) checking option. It may be enabled or disabled.
Retransmission time, max	Current time, in seconds, required to resend a packet and maximum time, in seconds, that was required to resend a packet since tunnel establishment.
Unsent queuesize, max	Current size of the unsent queue and maximum size of the unsent queue since tunnel establishment.

Table 51 show l2tun tunnel all Field Descriptions (continued)

Field	Description
Resend queuesize, max	Current size of the resend queue and maximum size of the resend queue since tunnel establishment.
Total resends	Total number of packets re-sent since tunnel establishment.
ZLB ACKs sent	Number of zero length body acknowledgment messages sent.
Total peer authentication failures	The total number of times peer authentication has failed.
Current nosession queue check	Number of tunnel timeout periods since the last session ended. Up to five tunnel timeouts are used if there are outstanding control packets on the unsent or resend queue. Otherwise, the tunnel is dropped after one tunnel timeout.
Retransmit time distribution	Histogram showing the number of retransmissions at 0, 1, 2,..., 8 seconds, respectively.
Sessions disconnected due to lack of resources	Number of sessions disconnected because of a lack of available resources.
secrets configured	The number of pseudowire control channel authentication passwords that are configured for the tunnel. One or two passwords may be configured.

The following example shows how to filter information to display L2TP control channel details only for the sessions configured with the local name Router and the remote name tun1:

```
Router# show l2tun tunnel transport local-name Router tun1

Tunnel Information Total tunnels 3 sessions 3

LocID Type Prot  Local Address   Port  Remote Address  Port
26515 IP   115   172.16.184.116  0     172.16.184.142  0
30866 IP   115   172.16.184.116  0     172.16.184.142  0
35217 IP   115   172.16.184.116  0     172.16.184.142  0
```

Table 52 describes the significant fields shown in the display.

Table 52 show l2tun tunnel transport Field Descriptions

Field	Description
Total tunnels	Total number of tunnels established.
sessions	Number of sessions established.
LocID	Local session ID.
Type	Session type.
Prot	Protocol type used by the tunnel.
Local Address	IP address of the local tunnel endpoint.
Port	Port used by the local tunnel endpoint.
Remote Address	IP address of the remote tunnel endpoint.
Port	Port used by the remote tunnel endpoint.

The following example shows how to display information about the current state of L2TP tunnels with the local and remote hostnames of each session:

```
Router# show l2tun tunnel state

LocID  RemID   Local Name Remote Name  State  Last-Chg
26515  41814   Router      tun1         est     03:13:15
30866  6809    Router      tun1         est     03:13:15
35217  37340   Router      tun1         est     03:13:15
```

Table 53 describes the significant fields shown in the display.

Table 53 show l2tun tunnel state Field Descriptions

Field	Description
LocID	Local session ID.
RemID	Remote session ID.
Local Name	Name of the local tunnel endpoint.
Remote Name	Name of the remote tunnel endpoint.
State	Current state of the tunnel.
Last-Chg	Time since the state of the tunnel last changed, in the format hh:mm:ss.

The following example shows the display of all possible L2TP control channel authentication AV pair statistics. AV pair statistic fields are displayed only if they are nonzero. For the purposes of this example, all possible output fields are displayed in the sample output.

This example is valid for Cisco IOS Release 12.0(31)S and later releases or Cisco IOS Release 12.2(27)SBC. To display authentication statistics in Cisco IOS Release 12.2(28)SB or a later release, use the **monitor l2tun counters tunnel l2tp** and **show l2tun counters tunnel l2tp** commands instead.

```
Router# show l2tun tunnel authentication

 L2TPv3 Tunnel Authentication Statistics:
   Nonce AVP Statistics:
     Ignored                              0
     Missing                              0
   All Digests Statistics:
     Unexpected                           0
     Unexpected ZLB                       0
   Primary Digest AVP Statistics:
     Validate fail                        0
     Hash invalid                         0
     Length invalid                       0
     Missing                              0
     Ignored                              0
     Passed                               0
     Failed                               0
   Secondary Digest AVP Statistics:
     Validate fail                        0
     Hash invalid                         0
     Length invalid                       0
     Missing                              0
     Ignored                              0
     Passed                               0
     Failed                               0
   Integrity Check Statistics:
     Validate fail                        0
```

```
    Length invalid                          0
    Passed                                  0
    Failed                                  0
  Local Secret Statistics:
    Missing                                 0
  Challenge AVP Statistics:
    Generate response fail                  0
    Ignored                                 0
  Challenge/Response AVP Statistics:
    Generate response fail                  0
    Missing                                 0
    Ignored                                 0
    Passed                                  0
    Failed                                  0
  Overall Statistics:
    Passed                                  0
    Skipped                                 0
    Ignored                                 0
    Failed                                  0
```

Table 54 describes the significant fields shown in the display.

Table 54 show l2tun tunnel authentication Field Descriptions

Field	Description
Nonce AVP Statistics	Counters for the nonce AV pair.
Ignored	Number of AV pair messages that were ignored.
Missing	Number of AV pair messages that were missing.
All Digests Statistics	Statistics for all configured digest passwords.
Unexpected	Digest information was received, but the router is not configured for it.
Unexpected ZLB	A ZLB message was received while control message authentication was enabled. ZLB messages are permitted only when control message authentication is disabled.
Primary Digest AVP Statistics	Statistics for AV pair messages that were exchanged using the primary L2TP Version 3 (L2TPv3) control message digest password.
Validate fail	Number of AV pair messages that failed to validate.
Hash invalid	Number of AV pair messages with an invalid hash.
Length invalid	Number of AV pair messages with an invalid length.
Passed	Number of AV pair messages that were successfully exchanged.
Failed	Number of AV pair messages that failed to authenticate.
Secondary Digest AVP Statistics	Statistics for AV pair messages that were exchanged using the secondary L2TPv3 control message digest password.
Integrity Check Statistics	Statistics for AV pair messages that were exchanged when integrity checking was enabled.
Local Secret Statistics	Statistics for AV pair that were messages related to the local secret.
Challenge AVP Statistics	Statistics for AV pair messages that were related to Challenge Handshake Authentication Protocol (CHAP), style authentication challenges.
Generate response fail	Number of AV pair messages that did not generate a response.

Table 54 show l2tun tunnel authentication Field Descriptions (continued)

Field	Description
Challenge/Response AVP Statistics	Statistics for AV pair messages exchanged when CHAP-style authentication is configured.
Overall Statistics	Summary of the statistics for all authentication AV pair messages.
Skipped	The number of AV pair messages that were not authenticated.

Related Commands

Command	Description
clear l2tun counters tunnel l2tp	Clears global or per-tunnel control message statistics for L2TP tunnels.
clear l2tun tunnel counters	Clears L2TP control channel authentication counters.
monitor l2tun counters tunnel l2tp	Enables or disables the collection of per-tunnel control message statistics for L2TP tunnels.
show l2tun	Displays general information about Layer 2 tunnels and sessions.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
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 l4f

To display the flow database for Layer 4 Forwarding (L4F), use the **show l4f** command in privileged EXEC mode.

show l4f {**clients** | **flows** [**brief** | **detail** | **summary**] | **statistics**}

Syntax Description

clients	Shows information about L4F clients.
flows	Shows information about L4F flows.
brief	(Optional) Shows brief information about L4F flows.
detail	(Optional) Shows detailed information about L4F flows.
summary	(Optional) Shows summary information about L4F flows.
statistics	Shows statistical information about L4F.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to examine the flow database for L4F. New statistics for L4F are available through this command. The per-flow statistics help to correlate the information with existing per-TCB statistics.

Examples

The following example displays the output of the **show l4f statistics** command. The fields in the table are self explanatory.

```
Router# show l4f statistics

L4F Global Statistics               Process     Interrupt

Client register                           4             0
Client deregister                         4             0
Client lookup failure                     8             0
Policy check accepted                     0             0
Policy check rejected                     0             0
Flows created                             0             0
Flow creation failed                      0             0
Flows destroyed                           0             0
Flows forced to bypass                    0             0
Flow lookup failed                        0             0
Flow cleanup scans                      501             0
Flows delayed for reinjection             0             0
Packet interception FORWARD               0             0
Packet interception PROXIED               0             0
Packet interception BYPASS                0             0
Packet interception ABORT                 0             0
Packet interception DROP                  0             0
Packet interception CONSUME               0             0
```

```
Packet interception PUNT                0            0
Packet interception UNKNOWN             0            0
Packet interception forced punt         0            0
Spoofing to proxying failures           0            0
Spoofing to proxying success            0            0
Spoofing to proxying timeouts           0            0
Read notify called                      0            0
Read notify aborted                     0            0
Read notify punt                        0            0
Read notify ok                          0            0
Read buffer                             0            0
Read packet                             0            0
Write notify called                     0            0
Write notify aborted                    0            0
Write notify punt                       0            0
Write notify ok                         0            0
Write buffer                            0            0
Write packet                            0            0
Close notify called                     0            0
Shutdown called                         0            0
Close called                            0            0
Abort called                            0            0
Spoofing mode packets                   0            0
Proxying mode packets                   0            0
Packet reinject state alloc fail        0            0
Packet buffer alloc failed              0            0
Packet reinjection                      0            0
Packet reinjection punts                0            0
Packet reinjection errors               0            0
Packet reinjection other                0            0
Packets delayed for reinjection         0            0
Packets drained from delay q            0            0
Packets freed from delay q              0            0
```

Related Commands

Command	Description
debug l4f	Enables troubleshooting for L4F flows.

show line x121-address

To display all the line and rotary group addresses that are in a router, use the **show line x121-address** command in user EXEC or privileged EXEC mode.

show line x121-address

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)YN	This command was introduced.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

You use this command to see whether any X.121 address has been assigned, and if so, to which line or rotary group it has been assigned.

Examples

The following example shows the lines and groups that have X.121 addresses. It also shows that address 1111 will be used as the calling address by calls originating from lines within Rotary Group 2.

```
Router# show line x121-address

   X121-Addresses     Line   Rotary
   34567              97      -
   12345              98      -
   23456              -       1
   1111               -       2 (calling-address)
```

Table 55 show line x121-address Field Descriptions

Field	Description
X121-Addresses	X.121 address assigned to the TTY line or rotary group identified to the right in the same row.
Line	The TTY line's absolute number.
Rotary	The rotary group's ID number. The words "calling address" also appear in this column when the group's X.121 address has been assigned to be the source address for all calls originating with members of that group.

Related Commands

Command	Description
show line	Displays status of configured lines.

show mace metrics

To display all Measurement, Aggregation, and Correlation Engine (MACE) metrics that were collected at the last export timeout, use the **show mace metrics** command in privileged EXEC mode.

show mace metrics [**summary** | [**name**] *monitor-name* [**art** | **waas**] | *source-ip* [*destination-ip* [*port* [*protocol*]]] [**art** | **waas**]]

Syntax Description

summary	(Optional) Displays the MACE metrics summary.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor of type MACE that was previously configured.
art	(Optional) Displays the Application Response Time (ART) metrics.
waas	(Optional) Displays the Wide Area Application Services (WAAS) metrics.
source-ip	(Optional) Source IP address used by the exported packets. You can specify a valid source IP address, or you can use the **any** keyword. If you use the **any** keyword, the command displays information about all the source IP addresses.
destination-ip	(Optional) IP address of the destination host. You can specify a valid destination IP address or use the **any** keyword. If you use the **any** keyword, the command displays information about all the destination IP addresses.
port	(Optional) Destination port to which the exported packets are sent. The range is from 1 to 65535. You can specify a valid port address, or you can use the **any** keyword. If you use the **any** keyword, the command displays information about all the ports.
protocol	(Optional) Transport layer protocol used by the exported packets. The range is from 1 to 256. You can specify a valid protocol, or you can use the **any** keyword. If you use the **any** keyword, the command displays information about all the protocols.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show mace metrics** command to display MACE metrics that are collected at the last export timeout. No metrics are displayed before the first export timeout. If you do not specify any source IP address, destination IP address, port, protocol, or flow-monitor, and instead use the **any** keyword, all MACE metrics for all flows are displayed.

Examples

The following examples are sample output from the **show mace metrics** command:

```
Router# show mace metrics summary
```

```
Segment          Client Pkts             Server Pkts             Flows Exported
0                 0                       0                       0
1                 618                     771                     155
2                 906                     890                     155
4                 0                       0                       0
8                 0                       0                       0
16                182                     181                     46
```

Table 56 describes the significant fields shown in the display.

Table 56 show mace metrics summary Field Descriptions

Field	Description
Segment	WAAS Segment ID.
Client Pkts	Number of packets that are sent by the client.
Server Pkts	Number of packets that are sent by the server.
Flows Exported	Number of flows that are exported in the previous interval.

```
Router# show mace metrics

Key fields:   | Client          | Server          | Dst. Port  | Protocol | Segment ID
MACE Metrics: | DSCP        AppId      cByte       cPkts       sByte       sPkts
ART Metrics:  | sumRT       sumAD       sumNT       sumCNT      sumSNT      sumTD
                sumTT       numT        sPkts       sByte       cPkts       cByte
                newSS       numR
WAAS Metrics: | optMode    InBytes     OutBytes    LZByteIn    LZByteOut   DREByteIn
                DREByteOut
Rec. 1    :   | 1.1.1.2         | 3.3.3.2         | 80         | 6        |  1
MACE Metrics: | 0           0          88           4           72          2
ART Metrics:  | 0         0          0          0          0          0          0
                0         2          0          4          0          0          0
WAAS Metrics: | 7         0          0          0          0          0          0
Rec. 2    :   | 1.1.1.2         | 3.3.3.2         | 80         | 6        |  2
MACE Metrics: | 0           0          152          6           72          2
ART Metrics:  | 0         0          0          0          0          0          0
                0         2          0          6          0          0          0
WAAS Metrics: | 7           0          0          0          0          0          0
```

Table 57 describes the significant fields shown in the display.

Table 57 show mace metrics Field Descriptions

Field	Description
Client	Client address.
Server	Server address.
Dst. Port	Destination server port.
Segment ID	WAAS segment ID.
DSCP	Differentiated Services Code Point (DSCP) value in the Type of Service (TOS) field.
AppId	Network-Based Application Recognition (NBAR) application ID.

Table 57 show mace metrics Field Descriptions (continued)

Field	Description
cByte	Client bytes.
cPkts	Client packets.
sByte	Server bytes.
sPkts	Server packets
sumRT	Response time sum.
sumAD	Application delay sum.
sumNT	Network time sum.
sumCNT	Client network time sum.
sumSNT	Server network time sum.
sumTD	Total delay sum.
sumTT	Transaction time sum.
numT	Number of transactions.
newSS	Number of sessions.
numR	Number of responses.
optMode	WAAS optimization mode.
InBytes	WAAS input bytes.
OutBytes	WAAS output bytes.
LZByteIn	WAAS Lempel-Ziv (LZ) input bytes.
LZByteOut	WAAS LZ output bytes.
DREByteIn	WAAS Data Redundancy Elimination (DRE) input bytes.
DREByteOut	WAAS DRE output bytes.

Related Commands

Command	Description
flow monitor type mace	Configures a Flexible NetFlow flow monitor of type MACE.
mace enable	Applies the global MACE policy on an interface.
mace monitor waas	Enables MACE on WAAS.

show mpls l2transport checkpoint

To display checkpointing information about Any Transport over MPLS (AToM) virtual circuits (VCs), use the **show mpls l2transport checkpoint** command in privileged EXEC mode.

show mpls l2transport checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The output of the commands varies, depending on whether the output reflects the active or standby Route Processor (RP).

On the active RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint

AToM Checkpoint info for active RP
Checkpointing is allowed
Bulk-sync checkpointed state for 1 VC
```

On the standby RP, the command displays the following output:

```
Router# show mpls l2transport checkpoint

AToM HA Checkpoint info for standby RP
1 checkpoint information block in use
```

In general, the output on the active RP shows that checkpointing information was sent to the backup RP. The output on the backup RP shows that checkpointing information was received from the active RP.

Related Commands

Command	Description
show mpls l2transport vc	Displays information about the checkpointed data when checkpointing is enabled.

show policy-map type mace

To display policy-map statistics for the Measurement, Aggregation, and Correlation Engine (MACE), use the **show policy-map type mace** command in privileged EXEC mode.

show policy-map type mace [*mace-name* [**class** *name*] | **apn** *number* | **interface** [*type number* [**vc** [*vpi/*]*vci* | **vp** *vpi* [*subinterface*]] [**input** [**class** *name*] | **output** [**class** *name*]] | **session** [**uid** [*session-id*]] [**input** [**class** *name*] | **output** [**class** *name*]]]

Syntax Description

mace-name	(Optional) Name of the policy map.
class *name*	(Optional) Displays quality of service (QoS) policy actions for an individual class map.
apn	(Optional) Displays Access Point Name (APN)-related policy information.
number	Number of the APN index. The range is from 1 to 65535.
interface	(Optional) Displays the interface on which the QoS policy is configured.
type number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
vc	(Optional) Displays the virtual circuit (VC) service policy.
vp	(Optional) Displays the virtual path (VP) service policy.
vpi/	(Optional) Virtual path identifier (VPI) of the VP. The range is 0 to 255.
vci	Virtual channel identifier (VCI) of the VC associated with this VP. The range is 1 to 65535.
subinterface	(Optional) Subinterface, where applicable. The accepted values for this field are: • cef-exception— Cisco Express Forwarding (CEF)-exception subinterface. • host—Host subinterface. • transit—Transit subinterface.
input	(Optional) Displays the input policy of the session.
output	(Optional) Displays the output policy of the session.
session	(Optional) Displays the QoS policy session.
uid	(Optional) Displays the session information based on the Subscriber Service Switch (SSS) unique ID.
session-id	(Optional) Unique ID of the session. The range is from 1 to 65535.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show policy-map type mace** command:

```
Router# show policy-map type mace mace_global

interface Ethernet1/0

Service-policy mace input: mace_global

Class-map: c1 (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: tcp any
0 packets, 0 bytes
5 minute rate 0 bps

Class-map: c2 (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: tcp any
0 packets, 0 bytes
5 minute rate 0 bps

Class-map: c3 (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: tcp any
0 packets, 0 bytes
5 minute rate 0 bps

Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

Table 58 describes the significant fields shown in the display.

Table 58 show policy-map type mace Field Descriptions

Field	Description
Service-policy	Displays the service policy that is configured as a traffic shaping policy within a policy map.
Class-map	Displays a class map configuration that is created to be used for matching packets to a specified class.

Related Commands

Command	Description
policy-map type mace	Configures a MACE policy map and enters policy-map configuration mode.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.

show smds addresses

To display the individual addresses and the interface they are associated with, use the **show smds addresses** privileged EXEC command.

show smds addresses

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 is sample output from the **show smds addresses** command:

```
Router# show smds addresses

SMDS address - Serial0   c141.5555.1212.FFFF
```

Table 59 describes the fields shown in the display.

Table 59 show smds addresses Field Descriptions

Field	Description
Serial0	Interface to which this SMDS address has been assigned.
c141.5555.1212	SMDS address that has been assigned to the interface.

show smds map

To display all Switched Multimegabit Data Service (SMDS) addresses that are mapped to higher-level protocol addresses, use the **show smds map** privileged EXEC command.

show smds map

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 is sample output from the **show smds map** command:

```
Router# show smds map

Serial0: ARP maps to e180.0999.9999.FFFF multicast
Serial0: IP maps to e180.0999.9999.FFFF 172.16.42.112 255.255.255.0 multicast
Serial0: IPX 1ABC.000.0c00.d8db maps to c111.1111.1111.1111 -- dynamic, TTL: 4 min
```

Table 60 describes the fields shown in the output.

Table 60 show smds map Field Descriptions

Field	Description
Serial0	Name of interface on which SMDS has been enabled.
ARP maps to	Higher-level protocol address that maps to this particular SMDS address.
e180.0999.9999.FFFF	SMDS address. Includes all SMDS addresses entered with either the **smds static-map** command (static) or **smds multicast** command (multicast).
172.16.42.112	IP address.
255.255.255.0	Subnet mask for the IP address.
static/dynamic	The address was obtained from a static map or dynamic map.
TTL	Time to live.

show smds traffic

To display statistics about Switched Multimegabit Data Service (SMDS) packets the router has received, use the **show smds traffic** privileged EXEC command.

show smds traffic

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 is sample output from the **show smds traffic** command:

```
Router# show smds traffic

624363 Input packets
759695 Output packets
2 DXI heartbeat sent
0 DXI heartbeat received
0 DXI DSU polls received
0 DXI DSU polls sent
0 DXI invalid test frames
0 Bad BA size errors
0 Bad Header extension errors
65 Invalid address errors
1 Bad tag errors
```

Table 61 describes the fields shown in the output.

Table 61 show smds traffic Field Descriptions

Field	Description
Input packets	Number of input packets.
Output packets	Number of output packets.
DXI heartbeat sent	Number of Data Exchange Interface (DXI) heartbeat polls transmitted.
DXI heartbeat received	Number of DXI heartbeat polls received.
DXI DSU polls sent	Number of DXI Data Service Unit (DSU) polls sent.
DXI DSU polls received	Number of DXI DSU polls received.
DXI invalid test frames	Number of invalid test frames seen.

Table 61 show smds traffic Field Descriptions (continued)

Field	Description
Bad BA size errors	Number of packets that have a size less than 32 or greater than 9188 bytes.
DXI Header extension errors	Number of extended SMDS Interface Protocol (SIP) Layer 3 header errors.
DXI Invalid address errors	Number of address errors.
Bad tag errors	Status indicating the number of errors that occur when there is a mismatch between the Tag value in the header and the BeTag value in the trailer of an SMDS frame. This usually indicates that there is a misconfiguration (that is, a DXI is connected to a non-DXI) or that the SMDS data service unit (SDSU) is scrambling the Layer 2 protocol data units (PDUs).

show srcp

To display Simple Resource Coordination Protocol (SRCP) information, use the **show srcp** command in user EXEC or privileged EXEC mode.

show srcp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following is sample output for **show srcp** command:

```
Router# show srcp

SRCP Admin State ACTIVE, Oper State ACTIVE
SRCP UDP port 2428
```

Table 62 describes the fields shown in the display.

Table 62 show srcp Field Descriptions

Field	Description
SRCP Admin State	Administrative state of the SRCP daemon.
Oper State	Operational state of the SRCP daemon.
SRCP UDP Port	The User Datagram Protocol (UDP) port used for the specified connection.

Related Commands

Command	Description
debug srcp	Enables debug traces for SRCP errors, events, media, packets, and parser.
srcp	Allocates resources for the SRCP and starts the daemon.

show vc-group

To display the names of all virtual circuit (VC) groups, use the **show vc-group** command in user EXEC or privileged EXEC mode.

show vc-group [*group-name*]

Syntax Description

group-name	(Optional) Name defined by the **vc-group** command. If this argument is not specified, the names of all VC groups in the system are displayed.

Defaults

The names of all VC groups in the system are displayed.

Command Modes

User EXEC
Privileged EXEC

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.

Examples

The following example shows the default display of the **show vc-group** EXEC command:

```
Router# show vc-group

Name of All VC Groups:
======================
network-1
```

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs, SVCs, and traffic information.
show frame-relay pvc	Displays statistics about Frame Relay interfaces.
vc-group	Assigns multiple Frame Relay DLCIs to a VC group.

show vfi

To display information related to a virtual forwarding instance (VFI), use the **show vfi** command in privileged EXEC mode.

Command Syntax in Releases 12.0(31)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SRB, and 12.2SX

show vfi *vfi-name*

Command Syntax in Release 12.2(33)SRC

show vfi name *vfi-name*

Command Syntax in Release 12.2(33)SRE

show vfi [**checkpoint** [**summary**] | **mac static address** | **memory** [**detail**] | **name** *vfi-name* [**checkpoint** | **mac static address**] | **neighbor** *ip-addr* **vcid** *vcid* **mac static address**]

Syntax Description

vfi-name	(Optional) Name of a specific VFI.
checkpoint	(Optional) Displays VFI checkpoint information.
summary	(Optional) Displays a summary of VFI checkpoint information.
mac	(Optional) Displays MAC address data.
static	(Optional) Displays static MAC address data.
address	(Optional) Displays static MAC addresses in a bridge domain.
memory	(Optional) Displays VFI memory usage.
detail	(Optional) Displays details of VFI memory usage.
name	(Optional) Displays the name of a specific VFI.
neighbor	(Optional) Displays VFI neighbor information.
ip-addr	(Optional) IP address of the neighbor (remote peer).
vcid	(Optional) Displays the virtual circuit ID for a peer.
vcid	(Optional) Integer from 1 to 4294967295 that identifies the virtual circuit.

Command Modes

Privileged EXEC (#)

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.
12.2(33)SRA	This command was updated to display the Virtual Private Network (VPN) ID.
12.2(33)SRB	This command was updated to display virtual private LAN service (VPLS) autodiscovery information.
12.2(33)SRC	This command was modified. The **name** keyword was added.

Release	Modification
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)SRE	This command was modified. The command syntax was changed, and support was added for the following keywords: **address**, **checkpoint**, **detail**, **mac**, **memory**, **neighbor**, **static**, **summary**, and **vcid**. Support was also added for the following arguments: *ip-addr* and *vcid*.

Usage Guidelines

Use this command to verify VFI configurations and for troubleshooting.

Examples

This example shows status for a VFI named VPLS-2. The virtual circuit ID in the output represents the VPN ID; the virtual circuit is identified by the combination of the destination address and the virtual circuit ID.

```
Router# show vfi VPLS-2

VFI name: VPLS-2, state: up
  VPN ID: 100
  Local attachment circuits:
    Vlan2
  Neighbors connected via pseudowires:
  Peer Address     VC ID     Split-horizon
  10.1.1.1          2             Y
  10.1.1.2          2             Y
  10.2.2.3          2             N
```

Table 63 describes the significant fields shown in the display.

Table 63 show vfi Field Descriptions

Field	Description
VFI name	The name assigned to the VFI.
state	The status of the VFI (up or down).
Local attachment circuits	The interface or VLAN assigned to the VFI.
Peer Address	The IP address of the peer router.
VC ID	The virtual circuit ID assigned to the pseudowire.
Split-horizon	Whether split horizon is enabled (Y) or disabled (N).

For the VPLS autodiscovery feature, the command output from the **show vfi** command includes autodiscovery information, as shown in the following example:

```
Router# show vfi

Legend: RT= Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: VPLS1, state: up, type: multipoint
  VPN ID: 10, VPLS-ID: 9:10
  RD: 9:10, RT: 10.10.10.10:150
  Local attachment circuits:
```

```
    Ethernet0/0.2
  Neighbors connected via pseudowires:
  Peer Address      VC ID       Discovered Router ID       S
  10.7.7.1           10          10.7.7.1                  Y
  10.7.7.2           10          10.1.1.2                  Y
  10.7.7.3           10          10.1.1.3                  Y
  10.7.7.4           10          10.1.1.4                  Y
  10.7.7.5           10          -                         Y

VFI name: VPLS2 state: up, type: multipoint
  VPN ID: 11, VPLS-ID: 10.9.9.9:2345
  RD: 10:11, RT: 10.4.4.4:151
  Local attachment circuits:
    Ethernet0/0.3
  Neighbors connected via pseudowires:
  Peer Address      VC ID       Discovered Router ID      S
  10.7.7.1           11          10.7.7.1                 Y
  10.7.7.2           11          10.1.1.5                 Y
```

Table 64 describes the significant fields in the output related to VPLS autodiscovery.

Table 64 show vfi Field Descriptions for VPLS Autodiscovery

Field	Description
VPLS-ID	The identifier of the VPLS domain. VPLS autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
RD	The route distinguisher (RD) to distribute endpoint information. VPLS autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID.
RT	The route target (RT). VPLS autodiscovery automatically generates a route target using the lower 6 bytes of the RD and VPLS ID.
Discovered Router ID	A unique identifier assigned to the PE router. VPLS autodiscovery automatically generates the router ID using the Multiprotocol Label Switching (MPLS) global router ID.

This example shows output from the **show vfi** command using the **memory** and **detail** keywords and the command syntax for Cisco IOS Release 12.2(33)SRE:

```
Router# show vfi memory detail

  VFI memory                  In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------

  VFI structs                 In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  vfi_context_t          :        --        --/--           --    52   --/--
  vfi_circuit_retry      :        --        --/--           --    24   --/--

  Total allocated: 0.000 Mb, 0 Kb, 0 bytes
```

Table 65 describes the significant fields in the output from the command using the **memory** and **detail** keywords.

Table 65 show vfi Field Descriptions in Cisco IOS Release 12.2(33)SRE

Field	Description
VFI memory	Amount of memory available for use.
In-use	Amount of memory actively used.
Asked-For/Allocated	Amount of memory originally requested/amount of memory allocated.
Count	Number of pieces of this named memory that exist.
Size	Size of the memory allocated by the system for this chunklet.
Config/Max	Number of chunklets per chunk.
VFI structs	Data structures being used.
Total allocated	Total allocated memory.

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

show waas alarms

To display WAAS Express status and alarms, use the **show waas alarms** command in privileged EXECmode.

show waas alarms

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display the status of the WAAS Express device and display the alarms that are enabled in the system.

Examples

The following output from the **show waas alarms** command shows that the alarms are turned on when the WAAS Express feature license has expired:

```
Router> enable
Router# show waas alarms

Alarms
    Connection limit exceeded:              off
    Too many peers discovered:              off
    WAAS license expired:                   off
    WAAS license revoked:                   off
    WAAS license deleted:                   on
    High CPU:                               off
```

Table 66 describes the significant fields shown in the display.

Table 66 show waas alarms Field Descriptions

Field	Description
Connection limit exceeded	Device exceeds the connection limit.
Too many peers discovered	Device exceeds the peer limit.
WAAS license expired	WAAS Express license has expired.
WAAS license revoked	WAAS Express license is revoked.
WAAS license deleted	WAAS Express license is deleted.
High CPU	CPU reaches maximum utilization.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
debug waas	Displays debugging information for different WAAS Express modules.
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.
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.

show waas auto-discovery

To display autodiscovery information for the WAAS Express device, use the **show waas auto-discovery** command in privileged EXEC mode.

show waas auto-discovery {**list** | **blacklist**}

Syntax Description

list	Displays the relevant autodiscovery states for the current connections.
blacklist	Displays the autodiscovery blacklist including the server address and state (grey or black).

Command Default

Autodiscovery information for the WAAS Express device is displayed with the associated connection states.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display connections being optimized and connections on which optimization is being negotiated.

Examples

The following is sample output from the **show waas auto-discovery list** command:

```
Router> enable
Router# show waas auto-discovery list

E: Established, S: Syn, A: Ack, F: Fin, R: Reset M: eMbryonic
s: sent, r: received, O: Options, P: Passthrough
    Src-IP:Port           Dst-IP:Port           Orig-St    Term-St
    192.168.111.111:65531 192.168.200.200:65531 Sr         SOs
```

Table 67 describes the significant fields shown in the display.

Table 67 show waas auto-discovery list Field Descriptions

Field	Description
Src-IP:Port	Source IP port number
Dst-IP:Port	Destination IP port number
Orig-St	Originating state
Term-St	Terminating state

The following is sample output from the **show waas auto-discovery blacklist** command:

```
Router> enable
Router# show waas auto-discovery blacklist

       Server IP                    Insert Time               State
       192.168.111.111:65531        Tue Jul 27 16:16:19 2010  Grey
```

Table 68 describes the significant fields shown in the display.

Table 68 show waas auto-discovery blacklist Field Descriptions

Field	Description
Server IP	The server address.
Insert Time	The blacklist insert time.
State	• Grey indicates that one acknowledgment was received without option 33. Grey also indicates that WAAS Express is in the validation state to add the IP address to the blacklist. • Black indicates that two acknowledgments were received without option 33. Black also indicates that packets are dropped with WAAS Express TCP options and are added to the blacklist. This enables WAAS Express to perform optimization.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
debug waas	Displays debugging information for different WAAS Express modules.
show waas alarms	Displays WAAS Express status and alarms.
show waas connection	Displays information about WAAS Express connections.
show waas statistics aoim	Displays WAAS Express peer information and negotiated capabilities.
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.

Command	Description
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.

show waas connection

To display WAAS Express connection details, use the **show waas connection** command in privileged EXEC mode.

show waas connection [**closed**] [**conn-id** *conn-id*] [**client-ip** *client-ip*] [**client-port** *client-port*] [**server-ip** *server-ip*] [**server-port** *server-port*] [**peer-id** *peer-id*] [**brief** | **detailed**]

Syntax Description

closed	(Optional) Displays the list of closed connections.
conn-id *conn-id*	(Optional) Displays connection information based on the connection ID.
client-ip *client-ip*	(Optional) Displays connection information based on client details.
client-port *client-port*	(Optional) Displays connection information based on client port details.
server-ip *server-ip*	(Optional) Displays connection information based on server details.
server-port *server-port*	(Optional) Displays connection information based on server port details.
peer-id *peer-id*	(Optional) Displays connection information based on peer details.
brief	(Optional) Displays information in brief format.
detailed	(Optional) Displays information in detailed format.

Command Default

For each connection, the following is displayed:

- Connection ID
- Destination IP address and port number
- Negotiated policies
- Peer ID
- Source IP address and port number

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display the following WAAS Express connection::

- The client and server information.
- The compression used to optimize the traffic.
- The time when the connection was initiated and closed.
- The reason for closing the connection.

Examples

The following is sample output from the **show waas connection** command:

```
Router> enable
Router# show waas connection

ConnID  Source IP:Port        Dest IP:Port          PeerID            Accel
1       192.168.20.99:51558   192.168.40.99:80      0021.5586.13df    TLD
```

Table 69 describes the significant fields shown in the display.

Table 69 show waas connection Field Descriptions

Field	Description
ConnID	The connection ID.
Source IP:Port	The source IP address and port number.
Dest IP:Port	The destination IP address and port number.
PeerID	The peer ID.

The following is sample output from the **show waas connection brief** command:

```
Router> enable
Router# show waas connection brief

Connection ID:                12345
    Peer Id:                  11:22:33:44:55:66
    Connection Type:          External Server
    Start Time:               Mar 10 15:10:30 2009
    Source IP Address:        192.168.111.111
    Source Port Number:       65535
    Destination IP Address:   192.168.111.111
    Destination Port Number:  65535
    Application Name:         web
    Classifier Name:          http
    Negotiated Policy:        LZ, DRE
    Accelerators:             TFO Only
    Orig-St                   ESTABLISHED
    Term-St                   ESTABLISHED
    Bytes Read Orig:          2147483648
    Bytes Written Orig:       2147483648
    Bytes Read Opt:           1610612736
    Bytes Written Opt:        1610612736
    TFO EOT State:            CONN_CLOSE
    TFO EOT:                  RS AR RR AS LFS
```

Table 70 describes the significant fields shown in the display.

Table 70 show waas connection brief Field Descriptions

Field	Description
Connection ID	Connection ID.
Peer Id:	Peer ID.
Connection Type:	External server and external client.
Start Time:	First synchronization received.
Source IP Address:	The source IP address.

Table 70 show waas connection brief Field Descriptions (continued)

Field	Description
Source Port Number:	The source IP port number.
Destination IP Address:	The destination IP address.
Destination Port Number:	The destination IP port number.
Application Name:	The application used for connection. This is web.
Classifier Name:	The name of the class-map that matches this flow.
Negotiated Policy:	The negotiated policy, such as LZ or DRE.
Accelerators:	The accelerators in the connection. In this example, it is TFO Only.
Orig-St	Originating state.
Term-St	Terminating state.
Bytes Read Orig:	Bytes received on the unoptimized side (LAN).
Bytes Written Orig:	Bytes sent on the unoptimized side.
Bytes Read Opt:	Bytes received on the optimized side (WAN).
Bytes Written Opt:	Bytes sent on the optimized side (WAN).
TFO EOT State:	State of closed connection between two WAAS peers.

The following is sample output from the **show waas connection detailed** command:

```
Router> enable
Router# show waas connection detailed

connection  ID:                          100
Peer Id:                                 0021.5586.1399
Connection Type:                         External
Start Time:                              01:41:54 UTC Jun 16 2010
End Time :                              01:41:59 UTC Jun 16 2010
End Reason:                              Closed
Source IP Address:                       192.168.21.99
Source Port Number:                      50894
Destination IP Address:                  192.168.41.99
Destination Port Number:                 80
Application Name:                        Web
Classifier Name:                         HTTP
Peer Policy:                             TFO, LZ, DRE
Configured Policy:                       TFO, LZ, DRE
Negotiated Policy:                       TFO, LZ, DRE
Accelerators:                            TFO ONLY
Bytes Read Orig:                         166
Bytes Written Orig:                      4577563
Bytes Read Opt:                          299867
Bytes Written Opt:                       1240
Auto-discovery information:
    Orig-St                              E
    Term-St                              EO
TFO information:
    TFO Frames Read:                     81
    TFO Frames Written:                  1
LZ section

    Encode stats
```

```
        Bytes in                    0
        Bytes out                   0
        Bypass bytes                209
        Compression gain            0%
        Avg Latency in Cef          0 usec
        Avg Latency in Proc         15 usec

    Decode stats
        Bytes in                    298613
        Bytes out                   4250094
        Bypass bytes                94
        Compression gain            92%
        Avg Latency in Cef          3 usec
        Avg Latency in Proc         407 usec
DRE section

    Encode stats
        Bytes in                    0
        Bytes out                   0
        Bypass bytes                166
        Compression gain            0%
        Avg latency                 0 usec

    Decode stats
        Bytes in                    4250147
        Bytes out                   4613677
        Bypass bytes                0
        Compression gain            7%
        Avg latency                 993 usec
Connection Status:
    WAN-LAN Status:
        Pending Data Read  : 59640
        LAN window event pending (36114)
        Last read notification (59640) received 8 ms ago
        Last write attempted 4 ms ago
        Last window notification received 4 ms ago
        Last attempted len : 17976
        Last error         : 11
        Last bytes accepted: -1
    LAN-WAN Status:
        Pending Data Read  : 0
        Last read notification (166) received 2476 ms ago
        Last write attempted 36 ms ago
        Last window notification received 132 ms ago
        Last attempted len : 15
        Last error         : 0
        Last bytes accepted: 15
```

Table 71 describes the significant fields shown in the display.

Table 71 show waas connection detailed Field Descriptions

Field	Description
connection ID	Connection ID.
Peer Id:	The IP address of the peer.
Connection Type:	External server, external client, internal server, and internal client.
Start Time:	First synchronization received.
End Time:	Last synchronization received.

Table 71 show waas connection detailed Field Descriptions (continued)

Field	Description
End Reason:	The reason why the synchronization ended.
Source IP Address:	The source IP address.
Source Port Number:	The source IP port number.
Destination IP Address:	The destination IP address.
Destination Port Number:	The destination IP port number.
Application Name:	The application used for connection. This is web.
Classifier Name:	The protocol used in the application. This is normally http.
Peer Policy:	The peer policy.
Configured Policy:	The configured policy.
Negotiated Policy:	The negotiated policy, such as LZ or DRE.
Accelerators:	The accelerators in the connection. In this example, it is TFO Only.
Orig-St	Originating state.
Term-St	Terminating state.
Bytes Read Orig:	Bytes received on the non optimized side (LAN).
Bytes Written Orig:	Bytes sent on the non optimized side.
Bytes Read Opt:	Bytes received on the optimized side (WAN).
Bytes Written Opt:	Bytes sent on the optimized side (WAN).
LZ section	Displays LZ compression/decompression statistics.
Encode stats Bytes in Bytes out	Displays the number of bytes encoded using the LZ compression and resulting output bytes.
Encode LZ Bypass Bytes	Number of bytes that bypassed the LZ module due to low compressibility.
Encode Avg Latency	The interval of number of bytes encoded using the LZ compression.
Decode Bytes in Bytes out	Displays the number of bytes decoded using the DRE compression and resulting output bytes.
Decode LZ Bypass Bytes	Number of bytes that bypassed by the LZ module due to low compressibility.
Decode Avg Latency	The interval of number of bytes decoded using the LZ compression
DRE section	Displays DRE compression/decompression statistics
Decode Avg latency	The interval of number of bytes encoded using the DRE compression.

Table 71 show waas connection detailed Field Descriptions (continued)

Field	Description
WAN-LAN Status:	Displays the connection status between the WAN and LAN interfaces.
Pending Data Read:	The number of bytes that are yet to be read.
LAN window event pending	The number of bytes that are yet to be processed by the LAN window event.
Last read notification received	The milliseconds since the notification was sent about the bytes that was read.
Last write attempted	The milliseconds since the byte sent was written.
Last window notification received	The milliseconds since the window notification was received.
Last attempted len:	The byte length that was attempted to write.
Last error:	The error that occurred while writing the bytes.
Last bytes accepted:	The last byte that was accepted.
LAN-WAN Status:	Displays connection status between the LAN and WAN interfaces.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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 statistics aoim	Displays WAAS Express peer information and negotiated capabilities.
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.

Command	Description
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.

show waas statistics aoim

To display WAAS Express peer information and negotiated capabilities, use the **show waas statistics aoim** command in privileged EXEC mode.

show waas statistics aoim

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays information about the peer and the negotiations.

Examples

The following example shows how to display WAAS peer information and negotiated capabilities:

```
Router> enable
Router# show waas statistics aoim

Total number of peer syncs:                     1
Current number of peer syncs in progress:       0
Number of peers:                                1
Number of local application optimizations (AO): 1
Number of AO discovery successful:              1
Number of AO discovery failure:                 0

Local AO statistics
AO type:                                        TFO
Total number of incompatible connections:       0

Peer AOIM Statistics
Number of Peers :                               1
Peer:                                           0021.5586.13df
Peer IP:                                        40.0.0.2
Peer Expiry Time:                               00:12:28
Peer Compatible:                                Yes
Peer active connections:                        0
Peer Aoim Version:                              1.0
Peer sync in progress:                          FALSE
Peer valid:                                     Yes
Peer Software Version:                          4.2.1(b31)
```

Table 72 describes the significant fields shown in the display.

Table 72 show waas statistics aoim Field Descriptions

Field	Description
Total number of peer syncs	Total number of peers synchronized.
Current number of peer syncs in progress	The number of peers for which synchronization is in progress.
Number of peers	The number of peers.
Number of local application optimizations (AO)	The number of local application optimizations (AOs) in the network
Number of AO discovery successful	The number of successful AOs.
Number of AO discovery failure	The number of failed AOs.
Local AO statistics	The statistics of the local AO.
AO type	The type of application optimization. In this case, it is TFO.
Total number of incompatible connections	The number of connections that were incompatible.
Peers:	Information about the peers.
Peer IP	The IP address of the peer.
Peer active connections	The number of active connections with the peer.
Peer sync in progress	Indicates peer synchronization in progress.
Peer valid	Indicates the validity of the entry in the peer table.
Peer Software Version	The software version in the peer system.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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 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.

Command	Description
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.

show waas statistics application

To display WAAS Express policy application statistics, use the **show waas statistics application** command in privileged EXEC mode.

show waas statistics application [**app-name** *app-name*]

Syntax Description

app-name *app-name*	(Optional) Displays statistics for a specific WAAS policy application.

Command Default

Statistics are displayed for all WAAS policy applications.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display statistical information about the WAAS policies.

Examples

The following is sample output from the **show waas statistics application** command::

```
Router> enable
Router# show waas statistics application waas-default

Application:     waas-default
TCP Data Volumes
Connection Type     Inbound                              Outbound
Opt TCP Plus        5054526                              13969693
Orig TCP Plus       35202552                             35202552
Opt TCP Only        0                                           0
Orig TCP Only       0                                           0
Internal Client     0                                           0
Internal Server     0                                           0

TCP Connection Counts
Connection Type     Active               Completed
Opt TCP Plus        0                           18
Opt TCP Only        0                            0
Internal Client     0                            0
Internal Server     0                            0

Pass Through Connection Counts
Connection Type     Completed
PT Asymmetric       0
PT Capabilities     0
PT Intermediate     0
PT_Other            0
Connection Reset:   0
Cleared connections 0
```

Table 73 describes the significant fields shown in the display.

Table 73 show waas statistics application Field Descriptions

Field	Description
Opt TCP Plus Bytes	Inbound/outbound optimized (WAN) TCP bytes.
Opt TCP Plus Packets	Inbound/outbound optimized (WAN) TCP packets.
Orig TCP Plus Bytes	Inbound/outbound originating (LAN) TCP bytes.
Orig TCP Plus Packets	Inbound/outbound originating (LAN) TCP packets.
Opt TCP Only Bytes	Inbound/outbound optimized (WAN) TCP bytes.
Opt TCP Only Packets	Inbound/outbound optimized (WAN) TCP packets.
Orig TCP Only Bytes	Inbound/outbound originating (LAN) TCP bytes.
Orig TCP Only Packets	Inbound/outbound originating (LAN) TCP packets
Internal Client Bytes	Packets terminating at the router where the router is a client.
Internal Server Bytes	Packets terminating at the router where the router is the server (WCM-NGWO).
Opt TCP Plus	Optimized TCP plus connection count.
Opt TCP Only	Optimized TCP only connection count.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.
PT Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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.

Command	Description
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.

show waas statistics auto-discovery

To display the autodiscovery statistics for a WAAS Express device, use the **show waas statistics auto-discovery** command in privileged EXEC mode.

show waas statistics auto-discovery [**blacklist**]

Syntax Description

blacklist	(Optional) Displays blacklist tables lookups, size, and the maximum hold time.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display statistics for autodiscovery states, success, and failures.

Examples

The following is sample output from the **show waas statistics auto-discovery** command:

```
Router> enable
Router# show waas statistics auto-discovery

Packets:
Total Sent:                          3
Total Received:                      3
Ack dropped in synack received state: 0
Non Syn dropped in nostate state:    0
Aoim sync syn-ack drop:              0
Aoim sync ack drop:                  0

Auto discovery failure:
Total Failure:                       0
Insufficient option space:           0
Invalid connection state:            0
Sequence number override:            0
Connection split failed:             0
Set sequence number failed:          0
Get sequence number failed:          0
Setting BIC failed:                  0
External module init failed:         0
Deleting options failed:             0
Set window size failed:              0
AOIM handover failed:                0
AOIM force sync failed:              0
AOIM peer addition failed:           0
AOIM synchronization reset:          0
TFO handover failed:                 0
Setting timestamp failed:            0
Setting window scale failed:         0
Setting send window failed:          0
```

```
Setting sack failed:                0
Setting keepalive failed:           0
FD association failed:              0

Auto discovery success SYN retransmission:
Zero retransmit:                    1
One retransmit:                     0
Two+ retransmit:                    0

Auto discovery Miscellaneous:
RST received:                       0
SYNs with our device id:            0
Zero device ID:                     0
Non standard option length:         0
Replication mode turned on:         0
ADM mode turned on:                 0
Capabilities mismatch:              0
Intermediate device:                0
Invalid option content:             0
Version mismatch:                   0
Peer AOIM incompatible:             0
Peer AOIM in progress:              0
AOIM peertable full:                0
AOIM multiple sync request passthrough:0
No peer:                            0
Missing Ack conf:                   0
```

Table 74 describes the significant fields shown in the display.

Table 74 show waas statistics auto-discovery Field Descriptions

Field	Description
Packets: Total Sent	Packets sent by autodiscovery.
Total Received	Packets received by autodiscovery.
Ack dropped in synack received state	Acknowledgment packet dropped within an AD state.
Non Syn dropped in nostate state	Nonsynchronization control packet dropped since no synchronization packet has been received.
Aoim sync syn-ack drop	Sychronization and acknowledgment dropped while AOIM synchronization is in progress.
Aoim sync ack drop	Acknowledgment dropped while AOIM synchronization is in progress.
Auto discovery failure: Total Failure	Number of failed flows.
Insufficient option space	Unable to add TCP options.
Invalid connection state	Connection state invalid.
Sequence number override	Sequence numbers out of sync.
Connection split failed	Unable to connect to a proxy.
Set sequence number failed	Sequence number bump failed.
Get sequence number failed	Unable to read sequence number.

Table 74 show waas statistics auto-discovery Field Descriptions (continued)

Field	Description
Setting BIC failed	Binary Increased Congestion Control (BIC) initialization failure.
External module init failed	Module initialization failure.
Deleting options failed	WAAS Express TCP option deletion failure.
Set window size failed	Window size adjustment failure.
AOIM handover failed	AOIM handover failure.
AOIM force sync failed	AOIM sync failure.
AOIM peer addition failed	AOIM peer could not be added.
TFO handover failed	TFO handover failure.
Setting timestamp failed	Unable to set the time stamp.
Setting window scale failed	Unable to set the windows scale.
Setting send window failed	Unable to set send the window on connection.
Setting sack failed	Unable to set the Selective Acknowledgment (SACK) on connection.
Setting keepalive failed	Failure to initialize keepalive.
FD association failed	Unable to associate file descriptor.
Auto discovery success SYN retransmission: Zero retransmit	Connections optimized for which a single synchronization was received.
One retransmit	Connections optimized for which a retransmitted synchronization was received.
Two+ retransmit	Two or more synchronization retransmissions.
Auto discovery Miscellaneous: RST received	Reset received during autodiscovery.
SYNs with our device id	Indicates synchronization with the WAAS Express device.
Zero device ID	Zero device ID advertised.
Non standard option length	Invalid WAAS Express TCP option.
Replication mode turned on	Connection bypass due to replication mode turned on.
ADM mode turned on	Connection bypass due to directed mode turned on.
Capabilities mismatch	Advertised capability mismatch.
Intermediate device	Intermediate WAAS Express device.
Invalid option content	Invalid WAAS Express TCP option.
Version mismatch	Administrative distance (AD) version mismatch.
Peer AOIM incompatible	Peer AOIM incompatible.
Peer AOIM in progress	Peer AOIM synchronization in progress.
AOIM peertable full	AOIM peer table full.

Table 74 show waas statistics auto-discovery Field Descriptions (continued)

Field	Description
AOIM multiple sync request passthrough	Pass through requested due to multiple simultaneous AOIM synchronization requests.
No peer	No peer for this connection.
Missing Ack conf	Missing autodiscovery confirmation.

The following is sample output from the **show waas statistics auto-discovery blacklist** command:

```
Router> enable
Router# show waas statistics auto-discovery blacklist

Auto-Discovery Blacklist Table Statistics
Operation Status:                       1
Total Lookups:                          0
Hits:                                   0
Miss (Grey Entry):                      0
Miss (No Entry):                        0
Table Insertions:                       0
Total Entries (Free & Used):            1024
Current Free Entries:                   1024
Current Used Entries:                   0
Peak Used Entries:                      0
Oldest Entry Hold Time (sec):           3600
IP Address Retrieval Failure:           0
Unexpected Threshold:                   0
```

Table 75 describes the significant fields shown in the display.

Table 75 show waas statistics auto-discovery blacklist Field Descriptions

Field	Description
Operation Status	Indicates whether the blacklist is enabled, which is 1.
Total Lookups	Total number of blacklist lookups.
Hits	Blacklist hits.
Miss (Grey Entry)	Hits in the grey list.
Miss (No Entry)	No blacklist found.
Table Insertions	Blacklist insertions.
Total Entries (Free & Used)	Total possible entries.
Current Free Entries	Free entries.
Current Used Entries	Used entries.
Peak Used Entries	Peak used entries.
Oldest Entry Hold Time (sec)	Active entry time period.
IP Address Retrieval Failure	Unable to locate IP address.
Unexpected Threshold	Invalid blacklist threshold.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
show waas statistics application	Displays WAAS Express policy application 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.

show waas statistics class

To display statistical information about the class in WAAS Express, use the **show waas statistics class** command in privileged EXEC mode.

show waas statistics class [**class-name** *class-name*]

Syntax Description

class-name *class-name*	(Optional) Specifies the class-name.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays statistical information about the class specified in WAAS Express. If a class name is not specified, the command displays the output for all the classes in WAAS Express.

Examples

The following is sample output from the **show waas statistics class** command:

```
Router> enable
Router# show waas statistics class

Number of Classes :             3
Class          FTP-Control
TCP Data Volumes
Connection Type     Inbound                              Outbound
Opt TCP Plus        0                                           0
Orig TCP Plus       0                                           0
Opt TCP Only        0                                           0
Orig TCP Only       0                                           0
Internal Client     0                                           0
Internal Server     0                                           0

TCP Connection Counts
Connection Type     Active               Completed
Opt TCP Plus        0                            0
Opt TCP Only        0                            0
Internal Client     0                            0
Internal Server     0                            0

Pass Through Connection Counts
Connection Type     Completed
PT Asymmetric       0
PT Capabilities     11
PT Intermediate     0
PT_Other            0
Connection Reset:   0

Class          waas-default
TCP Data Volumes
```

```
Connection Type     Inbound                           Outbound
Opt TCP Plus        0                                        0
Orig TCP Plus       0                                        0
Opt TCP Only        0                                        0
Orig TCP Only       0                                        0
Internal Client     0                                        0
Internal Server     0                                        0

TCP Connection Counts
Connection Type     Active               Completed
Opt TCP Plus        0                            0
Opt TCP Only        0                            0
Internal Client     0                            0
Internal Server     0                            0

Pass Through Connection Counts
Connection Type     Completed
PT Asymmetric       0
PT Capabilities     0
PT Intermediate     0
PT_Other            0
Connection Reset:   0

Class          FTP-Data
TCP Data Volumes
Connection Type     Inbound                           Outbound
Opt TCP Plus        722                                    573
Orig TCP Plus       0                                       24
Opt TCP Only        0                                        0
Orig TCP Only       0                                        0
Internal Client     0                                        0
Internal Server     0                                        0

TCP Connection Counts
Connection Type     Active               Completed
Opt TCP Plus        0                            4
Opt TCP Only        0                            0
```

Table 76 describes the significant fields shown in the display.

Table 76 show waas statistics class Field Descriptions

Field	Description
Class	The class name.
TCP Data Volumes	Indicates the volume of data in terms of connections, optimizations, and so on.
Connection Type	The type of connection.
Opt TCP Plus	Optimized TCP plus connection count.
Orig TCP Plus	Inbound/outbound originating TCP packets.
Opt TCP Only	Optimized TCP only connection count.
Orig TCP Only	Inbound/outbound originating TCP packets.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.

Table 76 show waas statistics class Field Descriptions (continued)

Field	Description
PT Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
show waas statistics application	Displays WAAS Express policy application statistics.
show waas statistics auto-discovery	Displays WAAS Express autodiscovery statistics.
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.

show waas statistics dre

To display Data Redundancy Elimination (DRE) statistics for a WAAS Express device, use the **show waas statistics dre** command in privileged EXEC mode.

show waas statistics dre [**peer**]

Syntax Description

peer	(Optional) Specifies the peer in the DRE.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display WAAS Express DRE statistics:

```
Router> enable
Router# show waas statistics dre

DRE Status:                                 Enabled

Cache
    Cache Status:                           Ready
    Oldest data age:                        00:07:35
    Total data storage size:                1468006400
    Total index size:                       11513600

WaitQ size:                                 0
WaitQ in storage:                           0

Connections
    Total:                                  24
    Active:                                 0

Encode Statistics
    Dre msgs:                               0
    Bytes in:                               0
    Bytes out:                              0
    Bypass bytes:                           14857511
    Compression gain:                       0%
    Average latency:                        2 usec

Decode Statistics
    Dre msgs:                               318
    Nacks generated:                        0
    Bytes in:                               8494760
    Bytes out:                              13780812
    Bypass bytes:                           35556
    Compression gain:                       38%
    Average latency:                        1471 usec

    Decode Message Size Distribution:
        0-1K   = 4              %
```

```
1-5K   = 0              %
5-15K  = 5              %
15-25K = 9              %
25-40K = 23             %
>40K   = 55             %
```

Table 77 describes the significant fields shown in the display.

Table 77 show waas statistics dre Field Descriptions

Field	Description
Cache:	Display DRE cache statistics.
Connection:	Total number of connection completed.
Message size distribution:	Indicates the distribution of messages across bytes in percentages.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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 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.

show waas statistics errors

To display error statistics for a WAAS Express device, use the **show waas statistics errors** command in privileged EXEC mode.

show waas statistics errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display WAAS Express Data Redundancy Elimination (DRE) statistics. The fields in the output are self-explanatory.

```
Router> enable
Router# show waas statistics errors

Unexpected EOT message:                       0
DRE message delayed for transmission:         0
Invalid input for TFO decode:                 0
RST ignored because EOT ACK sent:             0
RST ignored because EOT REQ sent:             0
Unknown TCP Control packet received:          0
DRE encode failed:                            0
Connection reset by peer:                     0
Connection timed out:                         0
No data to read:                              0
Buffer allocation failed:                     0
Error reading input particle:                 0
Error in semaphore acquisition:               0
Received control packet when expecting data:  0
Return value not handled:                     0
Lock condition:                               0
Out of transmit buffers:                      0
Error received from L4F:                      0
Error writing data:                           0
Error processing data:                        0
Error processing control packet:              0
Error sending data:                           0
Unable to find peer in table:                 0
```

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
debug waas	Displays debugging information for different WAAS Express modules.
show waas alarms	Displays WAAS Express status and alarms.

Command	Description
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.
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 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.

show waas statistics global

To display global statistics for a WAAS Express device, use the **show waas statistics global** command in privileged EXEC mode.

show waas statistics global

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display global statistics for a WAAS Express device:

```
Router> enable
Router# show waas statistics global

TCP Data Volumes
Connection Type           Inbound     Outbound
Opt TCP Plus              765708      2698
Orig TCP Plus             335         10486305
Opt TCP Only              0           0
Orig TCP Only             0           0
Internal Client           0           0
Internal Server           0           0

TCP Connection Counts
Connection Type           Active      Completed
Opt TCP Plus              0           2
Opt TCP Only              0           0
Internal Client           0           0
Internal Server           0           0

Pass Through Connection Counts
Connection Type                       Completed
PT Asymmetric                         0
PT Capabilities                       0
PT Intermediate                       0
PT_Other                              0
Connection Reset:                     1
Connection Closed:                    0
```

Table 78 describes the significant fields shown in the display.

Table 78 show waas statistics global Field Descriptions

Field	Description
TCP Data Volumes	Indicates the volume of data in terms of connections, optimizations, and so on.

Table 78 show waas statistics global Field Descriptions (continued)

Field	Description
Connection Type	The type of connection.
Opt TCP Plus	Optimized TCP plus connection count.
Orig TCP Plus	Inbound/outbound originating TCP packets.
Opt TCP Only	Optimized TCP only connection count.
Orig TCP Only	Inbound/outbound originating TCP packets.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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 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.

show waas statistics lz

To display the Lempel-Ziv compression statistics for a WAAS Express device, use the **show waas statistics lz** command in privileged EXEC mode.

show waas statistics lz

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display WAAS Express LZ statistics:

```
Router> enable
Router# show waas statistics lz

LZ Status:                          Enabled

Memory used                         30328 KB

Connections
    Total:                          75
    Active:                         0

Encode Statistics
    Bytes in:                       0
    Bytes out:                      0
    Bypass bytes:                   10886
    Compression gain:               0%
    Average latency in CEF path:    0 usec
    Average latency in process path:  293 usec
Decode Statistics
    Bytes in:                       25595
    Bytes out:                      71977
    Bypass bytes:                   776
    Compression gain:               64%
    Average latency in CEF path:    37 usec
    Average latency in process path:  9 usec
```

Table 79 describes the significant fields shown in the display.

Table 79 show waas statistics lz Field Descriptions

Field	Description
Memory used	Memory usage
Connections:	LZ connection statistics

Table 79 show waas statistics lz Field Descriptions (continued)

Field	Description
Encode Statistics	Displays the number of bytes encoded using the LZ compression, and the resulting output bytes.
Bypass bytes	Number of bytes that bypassed the LZ module due to low compressibility.
Compression gain	Compression gain achieve by encoding or decoding. This does not include bytes that LZ bypassed.
Average latency in CEF path	The interval, in milliseconds, between bytes encoded using the LZ compression.
Average latency in process path	The interval, in milliseconds, between bytes encoded using the LZ compression.
Decode Statistics	Displays the number of bytes decoded and the resulting output bytes.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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 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.

show waas statistics pass-through

To display the pass-through statistics for a WAAS Express device, use the **show waas statistics pass-through** command in privileged EXEC mode.

show waas statistics pass-through

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show waas statistics pass-through** command:

```
Router> enable
Router# show waas statistics pass-through

Pass Through Statistics:
Overall:                                1
No Peer:                                0
Rejected due to Capabilities:           0
Rejected due to Resources:              0
Interface Application config:           1
Interface Global config:                0
Asymmetric setup:                      0
Peer sync was in progress:              0
IOS WAAS is intermediate router:        0
Internal error:                         0
Other end is in black list:            0
AD version mismatch:                    0
Incompatable AO:                        0
Connection limit exceeded:              0
AOIM peertable full:                    0
AOIM multiple sync request passthrough: 0
Others:                                 0
```

Table 80 describes the significant fields shown in the display.

Table 80 show waas statistics pass-through Field Descriptions

Field	Description
Overall	Overall connection pass-through's.
No Peer	No peer found for the connection.
Rejected due to Capabilities	Pass-through due to mismatch of capabilities.
Rejected due to Resources	Pass-through due to lack of resources.
Interface Application config	Interface application pass-through.

Table 80 show waas statistics pass-through Field Descriptions (continued)

Field	Description
Interface Global config	Global configuration pass-through.
Asymmetric setup	Possible asymmetric setup.
Peer sync was in progress	Pass-through due to AOIM synchronization in progress.
IOS WAAS is intermediate router	Intermediate WAAS Express device.
Internal error	Internal error.
Other end is in black list	Blacklist passthrough.
AD version mismatch	Autodiscovery version mismatch.
Incompatable AO	Incompatible optimization.
Connection limit exceeded	Connection limited exceeded.
AOIM peertable full	Unable to add more AOIM peers.
AOIM multiple sync request passthrough	Pass through requested due to multiple simultaneous AOIM synchronization requests.
Others	Other conditions.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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 peer	Displays inbound and outbound statistics for peer WAAS Express devices.
show waas status	Displays the status of WAAS Express.

Command	Description
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.

show waas statistics peer

To display inbound and outbound statistics for peer Wide-area Application Engines (WAEs) devices, use the **show waas statistics peer** command in privileged EXEC mode.

show waas statistics peer [**id** *peer-id* [**conn**]]

Syntax Description

id *peer-id*	(Optional) Displays statistics for that peer ID.
conn	(Optional) Displays current optimized connections to that peer.

Command Default

Inbound and outbound statistics are displayed for all peer WAE devices. Current optimized connections are not displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display inbound and outbound statistics for all peer WAE devices.

Examples

The following is sample output from the **show waas statistics peer** command:

```
Router> enable
Router# show waas statistics peer

Number of Peers :         1
Peer:                     0021.5586.13df
TCP Data Volumes
Connection Type           Inbound        Outbound
Opt TCP Plus              765708         2698
Orig TCP Plus             335            10486305
Opt TCP Only              0              0
Orig TCP Only             0              0
Internal Client           0              0
Internal Server           0              0

TCP Connection Counts
Connection Type           Active         Completed
Opt TCP Plus              0              2
Opt TCP Only              0              0
Internal Client           0              0
Internal Server           0              0

Pass Through Connection Counts
Connection Type           Completed
PT Asymmetric             0
PT Capabilities           0
```

```
PT Intermediate           0
PT_Other                  0
Connection Reset:         1
Connection Closed:        0
```

Table 81 describes the significant fields shown in the display.

Table 81 show waas statistics peer Field Descriptions

Field	Description
Peer	MAC address of peer
TCP Data Volumes	Indicates the volume of data in terms of connections, optimizations, and so on.
Connection Type	The type of connection.
Opt TCP Plus	Inbound/outbound optimized (WAN) TCP bytes.
Orig TCP Plus	Inbound/outbound originating (LAN) TCP bytes.
Opt TCP Only	Inbound/outbound optimized (WAN) TCP bytes.
Orig TCP Only	Inbound/outbound originating (LAN) TCP bytes.
Internal Client	Packets terminating at the router where the router is a client.
Internal Server	Packets terminating at the router where the router is the server (WCM-NGWO).
Opt TCP Plus	Optimized TCP plus connection count.
Opt TCP Only	Optimized TCP only connection count.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.
PT Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
show waas statistics application	Displays WAAS Express policy application statistics.
show waas statistics auto-discovery	Displays WAAS Express autodiscovery statistics.

Command	Description
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 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.

show waas status

To display the status of Wide-Area Application Services (WAAS) Express, use the **show waas status** command in privileged EXEC mode.

show waas status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows the status of WAAS Express. The fields in the output are self-explanatory.

```
Router> enable
Router# show waas status

IOS Version: 15.1(20110128:013523)
WAAS Express Version: 1.1.0

WAAS Enabled Interface        Policy Map
FastEthernet8                 waas_global

WAAS Feature License
    License Type:                          Permanent

DRE Status                        : Enabled
LZ Status                         : Enabled + Entropy

Maximum Flows                     : 100
Total Active connections          : 0
Total optimized connections       : 0
```

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
show waas statistics application	Displays WAAS Express policy application statistics.

Command	Description
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 token	Displays the value of the configuration token used by the WAAS Central Manager.

show waas token

To display the value of the WAAS Express configuration token, use the **show waas alarms** command in privileged EXEC mode.

show waas token

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display the values of the WAAS Express configuration token.

Examples

The following is sample output from the **show waas token** command:

```
Router> enable
Router# show waas token

Config Token:1292
```

Table 82 describes the significant field shown in the display.

Table 82 show waas token Field Descriptions

Field	Description
Config Token	Monotonically increasing 32-bit number (unsigned integer).

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
show waas statistics application	Displays WAAS Express policy application statistics.

Command	Description
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.
waas cm-register url	Registers a device with the WAAS Central Manager.

show x25 context

To display operating configuration status details of an X.25 link, use the **show x25 context** command in privileged EXEC mode.

show x25 context [**xot** | **interface serial** *number* [**dlci** *number*] | *cmns-interface-type number* [**mac** *mac-address*]]

Syntax Description

xot	(Optional) Displays information specific to X.25 over TCP (XOT) contexts.
interface serial *number*	(Optional) Specific serial interface.
dlci *number*	(Optional) Specific data-link connection identifier (DLCI) link.
cmns-interface-type number	(Optional) Local Connection Mode Network Service (CMNS) interface type and number. CMNS interface types are Ethernet, Token Ring, and FDDI. The interface numbering scheme depends on the router interface hardware.
mac *mac-address*	(Optional) Hardware address of the CMNS interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	This command was modified to display information about X.25 failover.
12.2(8)T	The **xot** keyword was added to display information specific to XOT contexts.
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

XOT: Example

The following is sample output from the **show x25 context** command with the **xot** keyword:

```
Router# show x25 context xot

XOT Access-group 2
PROFILE mod128 station DXE/DTE, address 2222, state R1, modulo 128, timer 0
      Defaults: idle VC timeout 0
        input/output window sizes 80/80, packet sizes 256/256
      Timers: T20 180, T21 200, T22 180, T23 180
      RESTARTs 0/0 CALLs 5+0/7+0/0+0 DIAGs 0/0
XOT Access-group 3
station DXE/DTE, address <none>, state R1, modulo 8, timer 0
      Defaults: idle VC timeout 0
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T20 180, T21 200, T22 180, T23 180
      RESTARTs 0/0 CALLs 21+0/50+0/0+0 DIAGs 0/0
```

Serial Interface: Example

The following is sample output from the **show x25 context** command:

```
Router# show x25 context interface serial 1

Serial1 DLCI 20
PROFILE DCE, address <none>, state R1, modulo 8, timer 0
      Defaults: idle VC timeout 0
        input/output window sizes 2/2, packet sizes 128/128
      Timers: T10 60, T11 180, T12 60, T13 60
      Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
      RESTARTs 1/0 CALLs 0+0/0+0/0+0 DIAGs 0/0
  LAPB DCE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0
      VS 7, VR 6, tx NR 6, Remote VR 7, Retransmissions 0
      Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
      IFRAMEs 111/118 RNRs 0/0 REJs 0/0 SABM/Es 14/1 FRMRs 0/0 DISCs 0/0
```

X.25 Failover: Example

The following is sample output from the **show x25 context** command when the X.25 Failover feature is configured. The “Fail-over delay” field appears when the primary interface has gone down and come back up again. The number of seconds indicates the time remaining until the secondary interface will reset.

```
Router# show x25 context

Serial1 DLCI 33
  PROFILE dxe/DCE, address 3032, state R1, modulo 8, timer 0
      Defaults:idle VC timeout 0
        input/output window sizes 2/2, packet sizes 128/128
      Timers:T20 180, T21 200, T22 180, T23 180
      Channels:Incoming-only none, Two-way 1-4095, Outgoing-only none
      RESTARTs 12/0 CALLs 5+4/0+0/0+0 DIAGs 0/0
      Fail-over delay:16 seconds remaining on Dialer0
  LAPB dxe/DCE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0
      VS 1, VR 1, tx NR 1, Remote VR 1, Retransmissions 0
      Queues:U/S frames 0, I frames 0, unack. 0, reTx 0
      IFRAMEs 97/88 RNRs 0/0 REJs 0/0 SABM/Es 55490/12 FRMRs 186/0 DISCs
```

Table 83 describes significant fields shown in the displays.

Table 83 show x25 context Field Descriptions

Field	Description
XOT Access-group	Number of the XOT access group.
PROFILE	X.25 profile associated with the XOT access group.
address	Address to which the interface is connected.
state	State of the interface. Possible values are as follows: R1— normal ready state R2—DTE[1] restarting state R3—DCE[2] restarting state If the state is R2 or R3, the interface is awaiting acknowledgment of a Restart packet.
modulo	Modulo packet sequence numbering scheme.

Table 83 show x25 context Field Descriptions (continued)

Field	Description
timer	Interface timer value (zero unless the interface state is R2 or R3).
Defaults: idle VC timeout	Inactivity time before clearing the virtual circuit.
input/output window sizes	Default window sizes (in packets) for the interface. The **x25 facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
packet sizes	Default maximum packet sizes (in bytes) for the interface. The **x25 facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
Timers	Values of the X.25 timers are as follows: T10 through T13 for a DCE device T20 through T23 for a DTE device
Channels	Virtual circuit ranges for this interface.
RESTARTs	Restart packet statistics for the interface using the format Sent/Received.
CALLs	(number of successful calls sent + calls failed)/(calls received + calls failed)/(calls forwarded + calls failed). Calls forwarded are counted as calls sent.
DIAGs	Number of diagnostic messages sent and received.
Fail-over delay	Number of seconds remaining until secondary interface resets.

1. DTE = data terminal equipment
2. DCE = data communications equipment

Related Commands

Command	Description
show x25 profile	Displays information about configured X.25 profiles.
show x25 vc	Displays information about active X.25 virtual circuits.
x25 profile	Configures an X.25 profile without allocating any hardware-specific information.

show x25 cug

To display information about all closed user groups (CUGs) or specific CUGs (defined by the local or network CUG number), use the **show x25 cug** command in privileged EXEC mode.

show x25 cug {**local-cug** [*number*] | **network-cug** [*number*]}

Syntax Description

local-cug	Displays CUGs by locally significant CUG identifier.
number	(Optional) Local CUG number (0 to 9999). If you do not specify a CUG number, information for all CUGs will be displayed.
network-cug	Displays CUGs by network-translated CUG identifier.
number	(Optional) Network CUG number (0 to 9999). If you do not specify a CUG number, information for all CUGs will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	This command was modified to show information about CUG selection facility suppression.
12.2(13)T	This command was modified to display information about all or specific CUGs configured on terminal lines.
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

You must designate either the local CUG or the network CUG by the choice of keyword. Within that designation you can view all CUGs or a specific CUG defined by its local or network CUG identifier.

Examples

CUG Selection Facility Suppress Option: Example

The following is sample output for the **show x25 cug** command when CUG selection facility is suppressed for all CUGs on serial interface 1/2 and for the preferential CUG on the X.25 profile named "cug".

```
Router# show x25 cug local-cug

X.25 Serial1/2, 2 CUGs subscribed with no public access
  CUG selection facility suppressed for all CUGs
  local-cug 100 <-> network-cug 10
  local-cug 1 <-> network-cug 11
PROFILE cug, 2 CUGs subscribed with incoming public access
  CUG selection facility suppressed for preferential CUG
  local-cug 0 <-> network-cug 0 , preferential
```

```
  local-cug 100 <-> network-cug 100
  local-cug 200 <-> network-cug 200
```

Local CUG: Example

The following sample output from the **show x25 cug local-cug** command displays information about all local CUGs on configured on the router.

```
Router# show x25 cug local-cug

X.25 Serial1/1, 3 CUGs subscribed with no public access
  local-cug 99 <-> network-cug 9999, no-incoming, preferential
  local-cug 100 <-> network-cug 1000
  local-cug 101 <-> network-cug 1001
PROFILE cugs, 2 CUGs subscribed with with incoming public access
  local-cug 1 <-> network-cug 10, no-outgoing
  local-cug 2 <-> network-cug 20, no-incoming, preferential
Line: 129 aux 0  , 1 CUGs subscribed with outgoing public access
  local-cug 1 <-> network-cug 10
Line: 130 vty 0  , 4 CUGs subscribed with incoming and outgoing public access
  local-cug 1 <-> network-cug 10
  local-cug 50 <-> network-cug 5, preferential
  local-cug 60 <-> network-cug 6, no-incoming
  local-cug 70 <-> network-cug 7, no-outgoing
Line: 131 vty 1   , 1 CUGs subscribed with no public access
  local-cug 1 <-> network-cug 10
```

Network CUG: Example

The following is sample output from the **show x25 cug network-cug** command specifically for network number 10 showing that local CUG 1 is associated with it.

```
Router# show x25 cug network-cug 10

X.25 Serial1/2, 5 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
PROFILE cugs, 2 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1 , no-outgoing
Line: 129 aux 0   , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
Line: 130 vty 0   , 4 CUGs subscribed with incoming and outgoing public access
  network-cug 10 <-> local-cug 1
Line: 131 vty 1   , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
```

Table 84 describes the significant fields shown in the displays.

Table 84 show x25 cug Field Descriptions

Field	Description
X.25 Serial...	DCE interface with X.25 CUG service subscription.
PROFILE	X.25 profile with X.25 CUG service subscription.
Line	Terminal line with X.25 CUG service subscription.
local-cug	Local CUG details.
network-cug	Network CUG details.
preferential	Identifies which CUG, if any, is preferred. A single CUG listed for an interface is assumed to be preferred.

Related Commands

Command	Description
x25 subscribe cug-service	Enables and controls standard CUG behavior on an X.25 DCE interface.
x25 subscribe local-cug	Configures a DCE X.25 interface for a specific CUG subscription.

show x25 hunt-group

To display hunt groups and view detailed interface statistics and distribution methods, use the **show x25 hunt-group** command in privileged EXEC mode.

show x25 hunt-group [*name*]

Syntax Description

name	(Optional) Displays the specific hunt group named.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(5)T	The command output status field was modified to include “unoperational” as a type of interface status.
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 **clear counters** or the **clear x25** commands in EXEC mode to clear the count of VCs in use in the “status” field and the number of bytes of data transmitted and received in the “traffic” field. Since the “uses” field is a hunt-group-specific counter, it will not be cleared using the **clear counters** or **clear x25** commands. The “uses” field is only cleared at boot time or when the hunt group is defined.

Examples

The following is sample output from the **show x25 hunt-group** command:

```
Router# show x25 hunt-group

   ID      Type      Target                    uses      status    traffic(out/in)
 ================================================================================
 HG1       rotary    Serial1                   2         next      1158/1691
                     Serial2                   2         next      1328/2146
                     xot 172.17.125.54         2         last_used 137/3154
                     xot 172.17.125.34         1         next      137/3154


 HG2       vc-count  Serial2                   4         5 VCs     6921/1364
                     Serial3                   2         1 VC      70/1259
```

Table 85 describes significant fields shown in the display.

Table 85 show x25 hunt-group Field Descriptions

Field	Description
ID	Hunt group name.
Type	Method of load balancing (rotary or vc-count).
Target	Range of interfaces that a call within the hunt group can go to.
uses	Total number of call attempts (failed plus successful) made to the interface.
status	State of interface at that moment. The status of an interface may be one of the following: • next—Interface will be used next for rotary distribution method. • last used—Interface was just used for rotary distribution method. • unavailable—Interface is shutdown. • full—All logical channels on the interface are in use. • # VC—(vc-count only) Number of VCs currently in use on the interface. • unoper—All VCs on the interface are unoperational.
traffic (out/in)	Number of data bytes transmitted through the interface.

Related Commands

Command	Description
clear x25	Restarts an X.25 or CMNS service, clears an SVC, or resets a PVC.
x25 hunt-group	Creates and maintains a hunt group.

show x25 interface

To display information about virtual circuits (VCs) that use an X.25 interface and, optionally, about a specified virtual circuit, use the **show x25 interface** EXEC command.

show x25 interface [**serial** *number* | *cmns-interface* **mac** *mac-address*]

Syntax Description

serial *number*	(Optional) Keyword **serial** and number of the serial interface used for X.25.
cmns-interface **mac** *mac-address*	(Optional) Local CMNS interface type and number, plus the MAC address of the remote device. CMNS interface types are Ethernet, Token Ring, or FDDI. The interface numbering scheme depends on the router interface hardware.

Command Modes

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.

Examples

The following **show x25 interface** sample output displays X.25 information about VCs on serial interface 0:

```
Router# show x25 interface serial 0

SVC 1,  State: D1,  Interface: Serial0
  Started 00:13:52, last input 00:00:05, output never
  Connects 3334 <-> ip 3.3.3.4
  Call PID ietf, Data PID none
  Window size input: 7, output: 7
  Packet size input: 512, output: 512
  PS: 0  PR: 6  ACK: 1  Remote PR: 0  RCNT: 5  RNR: no
  P/D state timeouts: 0  timer (secs): 0
  data bytes 0/2508 packets 0/54 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
SVC 32,  State: D1,  Interface: Serial0.11
  Started 00:16:53, last input 00:00:37, output 00:00:28
  Connects 3334 <-> clns
  Call PID cisco, Data PID none
  Window size input: 7, output: 7
  Packet size input: 512, output: 512
  PS: 5  PR: 4  ACK: 4  Remote PR: 4  RCNT: 0  RNR: no
  P/D state timeouts: 0  timer (secs): 0
  data bytes 378/360 packets 21/20 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

show x25 map

To display information about configured address maps, use the **show x25 map** command in privileged EXEC mode.

show x25 map

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(8)T	This command was modified to display record boundary preservation information for address maps.
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 **show x25 map** command displays information about the following:

- Configured maps (defined by the **x25 map** command)
- Maps implicitly defined by encapsulation permanent virtual circuits (PVCs) (defined by the encapsulating version of the **x25 pvc** command)
- Dynamic maps (from the X.25 Defense Data Network [DDN] or Blacker Front End [BFE] operations)

Examples

Record Boundary Preservation: Examples

The following is sample output of the **show x25 map** command for a router that is configured with record boundary preservation (RBP) using the **x25 pvc rbp remote** command:

```
Router# show x25 map

Serial1/0:-> rbp, destination host 10.0.0.33 port 9999
  PVC, 1 VC:1/P
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 map rbp remote** command:

```
Router# show x25 map

Serial3/0:12132 -> rbp, destination host 10.0.0.32 port 9999
  permanent, 1 VC:1024
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 pvc rbp local** command:

```
Router# show x25 map

Serial3/0:<- rbp, listening at port 9999
  PVC, 1 VC:2/P
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 map rbp local** command:

```
Router# show x25 map

Serial1/0:12131 <- rbp, listening at port 9999
  permanent, 1 VC:1
```

Table 86 describes significant fields shown in the display.

Table 86 show x25 map Field Descriptions for Maps That Use Record Boundary Preservation

Field	Description
Serial1/0	Interface on which this map is configured.
12131	(For SVCs only) X.121 address of the remote host. If any call user data is configured, it will appear in this field also.
-> rbp	Indicates an outgoing TCP session that is configured to use RBP.
<- rbp	Indicates an incoming TCP session that is configured to use RBP.
destination host 10.0.0.32 port 9999	IP address and port number of the destination host for an outgoing TCP session.
listening at port 9999	Port number on which the router is listening for a TCP connection request for incoming TCP sessions.
permanent	Indicates that the address map was explicitly configured using the **x25 map rbp local** or **x25 rbp remote** command.
PVC	Indicates that the address map was created when a PVC was configured using the **x25 pvc rbp local** or **x25 pvc rbp remote** command.
1 VC:1	Number of circuits associated with the map, followed by a list of circuit numbers. /P indicates a PVC.

Typical X.25 Maps: Example

The following is sample output from the **show x25 map** for five maps that were configured with the **x25 map** command:

```
Router# show x25 map

Serial0: X.121 1311001 <--> ip 172.20.170.1
  PERMANENT, BROADCAST, 2 VCS: 3 4
Serial0: X.121 1311005 <--> appletalk 128.1
  PERMANENT
Serial1: X.121 2194441 cud hello <--> pad
  PERMANENT, windowsize 5 5, accept-reverse, idle 5
Serial1: X.121 1311005 <--> bridge
  PERMANENT, BROADCAST
Serial2: X.121 001003 <--> apollo 1.3,
         appletalk 1.3,
```

```
        ip 172.20.1.3,
        decnet 1.3,
        novell 1.0000.0c04.35df,
        vines 00000001:0003,
        xns 1.0000.0c04.35df,
        clns
PERMANENT, NVC 8, 1 VC: 1024
```

The display shows that five maps have been configured for a router: two for serial interface 0, two for serial interface 1, and one for the serial interface 2 (which maps eight protocols to the host).

Table 87 describes significant fields shown in the display.

Table 87 show x25 map Field Descriptions for Typical X.25 Maps

Field	Description
Serial0	Interface on which this map is configured.
X.121 1311001	X.121 address of the mapped encapsulation host.
ip 172.20.170.1	Type and address of the higher-level protocols mapped to the remote host. Bridge maps do not have a higher-level address; all bridge datagrams are sent to the mapped X.121 address. Connectionless Network Service (CLNS) maps refer to a configured neighbor as identified by the X.121 address.
PERMANENT	Address-mapping type that has been configured for the interface in this entry. Possible values include the following: • CONSTRUCTED—Derived with the DDN or BFE address conversion scheme. • PERMANENT—Map was entered with the **x25 map** interface configuration command. • PVC—Map was configured with the **x25 pvc** interface command.
BROADCAST	If any options are configured for an address mapping, they are listed; the example shows a map that is configured to forward datagram broadcasts to the mapped host.
2 VCs:	If the map has any active virtual circuits, they are identified.
3 4	Identifies the circuit number of the active virtual circuits. Note that a single protocol virtual circuit can be associated with a multiprotocol map.

show x25 profile

To view details of X.25 profiles on your router, use the **show x25 profile** command in privileged EXEC mode.

show x25 profile [*name*]

Syntax Description

name	(Optional) Name of X.25 profile.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(8)T	This command was modified to display the XOT access groups associated with an X.25 profile.
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 the X.25 profile name is not specified, the output shows all configured profiles for a given interface.

Examples

The following sample output from the **show x25 profile** command displays details about the X.25 profile called “XOT-DEFAULT”:

```
Router# show x25 profile XOT-DEFAULT

X.25 profile name: XOT-DEFAULT
In use by:
  Access-group 2
  Access-group 10
PROFILE dxe/DTE, address 12345, state R/Inactive, modulo 128, timer 0
Defaults: idle VC timeout 0
input/output window sizes 20/20, packet sizes 256/256
Timers: T20 180, T21 200, T22 180, T23 180
Channels: Incoming-only none, Two-way 1-4095, Outgoing-only none
```

The following sample output from the **show x25 profile** command displays all profiles configured on the same interface:

```
Router# show x25 profile

X.25 profile name:NetworkNodeA
  Number of references:2
  In use by:
      Annex G:Serial1 DLCI 20
      Annex G:Serial1 DLCI 30
```

```
  PROFILE DCE, address <none>, state R/Inactive, modulo 128, timer 0
      Defaults:idle VC timeout 5
        input/output window sizes 2/2, packet sizes 128/128
      Timers:T10 60, T11 180, T12 60, T13 60
      Channels:Incoming-only none, Two-way 1-128, Outgoing-only none
  LAPB DCE, modulo 8, k 7, N1 default, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0

X.25 profile name:NetworkNodeB
  Number of references:1
  In use by:
      Annex G:Serial1 DLCI 40
  PROFILE DTE, address 1111, state R/Inactive, modulo 8, timer 0
      Defaults:idle VC timeout 0
        input/output window sizes 2/2, packet sizes 128/128
      Timers:T20 180, T21 200, T22 180, T23 180
      Channels:Incoming-only none, Two-way 1-1024, Outgoing-only none
LAPB DTE, modulo 8, k 7, N1 default, N2 20
      T1 3000, T2 0, interface outage (partial T3) 0, T4 0
```

Table 88 describes significant fields shown in the display.

Table 88 show x25 profile Field Descriptions

Field	Description
Number of references	Number of X.25 connections using this profile.
In use by	Shows the interface, XOT access group, and X.25 service using this profile.
address	Address to which interface is connected.
state	State of the interface. Possible values are as follows: R1—normal ready state R2—DTE[1] restarting state R3—DCE[2] restarting state If the state is R2 or R3, the interface is awaiting acknowledgment of a Restart packet.
modulo	Value that determines the packet sequence numbering scheme used.
timer	Interface timer value (zero unless the interface state is R2 or R3).
Defaults: idle VC timeout	Inactivity time before clearing the virtual circuit.
input/output window sizes	Default window sizes (in packets) for the interface. The **x25 facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
packet sizes	Default maximum packet sizes (in bytes) for the interface. The **x25 facility** interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.

Table 88 show x25 profile Field Descriptions (continued)

Field	Description
Timers	Values of the X.25 timers are as follows: T10 through T13 for a DCE device T20 through T23 for a DTE device
Channels:	Virtual circuit ranges for this interface.

1. DTE = data terminal equipment
2. DCE = data communications equipment

Related Commands

Command	Description
show x25 context	Displays details of an Annex G DLCI link.
show x25 vc	Displays information about active X.25 virtual circuits.
x25 profile	Configures an X.25 profile without allocating any hardware-specific information.

show x25 remote-red

Note Effective with Cisco IOS Release 12.2, the **show x25 remote-red** command is not available in Cisco IOS Software.

To display the one-to-one mapping of the host IP addresses and the remote Blacker Front End (BFE) device's IP addresses, use the **show x25 remote-red** command in privileged EXEC mode.

show x25 remote-red

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	This command became unsupported.

Examples

The following is sample output from the **show x25 remote-red** command:

```
Router# show x25 remote-red

Entry       REMOTE-RED     REMOTE-BLACK   INTERFACE
1           21.0.0.3       21.0.0.7       serial3
2           21.0.0.10      21.0.0.6       serial1
3           21.0.0.24      21.0.0.8       serial3
```

Table 89 describes significant fields shown in the display.

Table 89 show x25 remote-red Field Descriptions

Field	Description
Entry	Address mapping entry.
REMOTE-RED	Host IP address.
REMOTE-BLACK	IP address of the remote BFE device.
INTERFACE	Name of interface through which communication with the remote BFE device will take place.

show x25 route

To display the X.25 routing table, use the **show x25 route** command in privileged EXEC mode.

show x25 route

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **dns** keyword was 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.

Examples

The following example shows output from the **show x25 route** command:

```
Router# show x25 route

# Match                     Substitute              Route To
1 dest ^1311001$                                    Serial0, 0 uses
2 dest ^1311002$                                    xot 172.20.170.10
3 dest 444                                          xot dns \0
4 dest 555                                          xot dns \0
```

Table 90 describes significant fields shown in the display.

Table 90 show x25 route Field Descriptions

Field	Description
#	Number identifying the entry in the X.25 routing table.
Match	The match criteria and patterns associated with this entry.
Route To	Destination to which the router will forward a call; X.25 destinations identify an interface; CMNS destinations identify an interface and host MAC address; XOT destinations either identify up to six IP addresses (#2), or the **x25 route** pattern for retrieving up to six IP addresses from the DNS (#3 and #4).

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).

show x25 services

To display information pertaining to the X.25 services, use the **show x25 services** command in user EXEC or privileged EXEC mode.

show x25 services

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
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

This command is the default form of the **show x25** command.

Examples

The following is sample output from the **show x25 services** command:

```
Router# show x25 services

X.25 software, Version 3.0.0.
  3 configurations supporting 3 active contexts
  VCs allocated, freed and in use: 7 - 0 = 7
  VCs active and idle: 4, 3
XOT software, Version 2.0.0.
  VCs allocated, freed and in use: 2 - 1 = 1
  connections in-progress: 0 outgoing and 0 incoming
  active VCs: 1, connected to 1 remote hosts
```

Related Commands

Command	Description
show x25 interface	Displays information about VCs that use an X.25 interface and, optionally, about a specified VC.
show x25 map	Displays information about configured address maps.
show x25 route	Displays the X.25 routing table.
show x25 vc	Displays information about active SVCs and PVCs.

show x25 vc

To display information about active switched virtual circuits (SVCs) and permanent virtual circuits (PVCs), use the **show x25 vc** command in privileged EXEC mode.

show x25 vc [*lcn*]

Syntax Description

lcn	(Optional) Logical channel number (LCN).

Command Modes

Privileged EXEC

Command History

Release	Modification
8.3	This command was introduced in a release prior to Release 8.3.
12.2(8)T	This command was modified to display information about record boundary preservation.
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

To examine a particular virtual circuit number, add an LCN argument to the **show x25 vc** command.

This command displays information about virtual circuits (VCs). VCs may be used for a number of purposes, such as the following:

- Encapsulation traffic
- Traffic switched between X.25 services (X.25, Connection-Mode Network Service [CMNS], and X.25 over TCP/IP [XOT])
- PAD traffic
- QLLC traffic

The connectivity information displayed will vary according to the traffic carried by the VC. For multiprotocol circuits, the output varies depending on the number and identity of the protocols mapped to the X.121 address and the encapsulation method selected for the circuit.

Examples

Record Boundary Preservation: Example

The following is sample output of the **show x25 vc** command for a PVC configured with record boundary preservation (RBP):

```
Router# show x25 vc

PVC 2,  State:D1,  Interface:Serial3/0
  Started 00:08:08, last input 00:00:01, output 00:00:01
  recordsize:1500, connected
  local address 10.0.0.1 port 9999; remote address 10.0.0.5 port 11029
  deferred ack:1
```

```
Window size input:2, output:2
Packet size input:128, output:128
PS:2  PR:2  ACK:1  Remote PR:2  RCNT:1  RNR:no
P/D state timeouts:0  timer (secs):0
data bytes 8000/8000 packets 80/80 Resets 9/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Table 91 describes the fields shown in the sample output that are typical for virtual circuits.

Table 91 show x25 vc Field Descriptions

Field	Description
SVC *n* or PVC *n*	Identifies the type of virtual circuit (switched or permanent) and its LCN (also called its "virtual circuit number").
State	State of the virtual circuit (which is independent of the states of other virtual circuits); D1 is the normal ready state. See the International Telecommunication Union Telecommunication Standardization Sector (ITU-T)[1] X.25 Recommendation for a description of virtual circuit states.
Interface	Interface or subinterface on which the virtual circuit is established.
Started	Time elapsed since the virtual circuit was created.
last input	Time of last input.
output	Time of last output.
Connects...<- ->..	Traffic-specific connection information. See Table 93, Table 94, Table 95, and Table 96 for more information.
D-bit permitted	Indicates that the X.25 D-bit (Delivery Confirmation) may be used on this circuit (displayed as needed).
Fast select VC	Indicates that the Fast Select facility was present on the incoming call (displayed as needed).
Reverse charged	Indicates reverse charged virtual circuit (displayed as needed).
Window size	Window sizes for the virtual circuit.
Packet size	Maximum packet sizes for the virtual circuit.
PS	Current send sequence number.
PR	Current receive sequence number.
ACK	Last acknowledged incoming packet.
Remote PR	Last receive sequence number received from the other end of the circuit.
RCNT	Count of unacknowledged input packets.
RNR	State of the Receiver Not Ready flag; this field is true if the network sends a Receiver-not-Ready packet.
Window is closed	This line appears if the router cannot transmit any more packets until the X.25 Layer 3 peer has acknowledged some outstanding packets.
P/D state timeouts	Number of times a supervisory packet (Reset or Clear) has been retransmitted.
Timer	A nonzero time value indicates that a control packet has not been acknowledged yet or that the virtual circuit is being timed for inactivity.
Reassembly	Number of bytes received and held for reassembly. Packets with the M-bit set are reassembled into datagrams for encapsulation virtual circuits; switched X.25 traffic is not reassembled (and is displayed only when values are not zero).

Table 91 show x25 vc Field Descriptions (continued)

Field	Description
Held Fragments/Packets	Number of X.25 data fragments to transmit to complete an outgoing datagram, and the number of datagram packets waiting for transmission (displayed only when values are not zero).
data bytes *m*/*n* packets *p*/*q*	Total number of data bytes sent (m), data bytes received (n), data packets sent (p), and data packets received (q) since the circuit was established.
Resets *t*/*r*	Total number of reset packets transmitted/received since the circuit was established.
RNRs *t*/*r*	Total number of Receiver Not Ready packets transmitted/received since the circuit was established.
REJs *t*/*r*	Total number of Reject packets transmitted/received since the circuit was established.
INTs *t*/*r*	Total number of Interrupt packets transmitted/received since the circuit was established.

1. The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

Table 92 describes the fields specific to VCs configured with record boundary preservation.

Table 92 show x25 vc Field Descriptions for VCs That Use Record Boundary Preservation

Field	Description
recordsize	Maximum record size for the session.
connected	Connection status.
local address; port	IP address and port number of the local end of the TCP session.
remote address; port	IP address and port number of the remote end of the TCP session.
input queue	Number of inbound X.25 data packets not yet processed. This field appears in the display only when the value is not zero.
record buffer	Number of bytes of X.25 data in the current partial record (not including data packets in the input queue). This field appears in the display only when the value is not zero.
deferred ack	Number of X.25 data packets that have been received and processed but not yet acknowledged. This field appears in the display only when the value is not zero.

Encapsulated Traffic: Example

The following is sample output of the **show x25 vc** command used on an encapsulated traffic circuit:

```
Router# show x25 vc 1024

SVC 1024, State: D1, Interface: Serial0
 Started 0:00:31, last input 0:00:31, output 0:00:31
 Connects 170090 <-->
    compressedtcp 172.20.170.90
    ip 172.20.170.90
 Call PID multi, Data PID ietf
 Reverse charged
```

```
Window size input: 2, output: 2
Packet size input: 128, output: 128
PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
Window is closed
P/D state timeouts: 0 Timer (secs): 0
 data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Table 93 describes the connection fields specific to encapsulation traffic.

Table 93 show x25 vc Encapsulation Traffic Field Descriptions

Field	Description
170090	The X.121 address of the remote host.
ip 172.20.170.90	The higher-level protocol and address values that are mapped to the virtual circuit.
Call PID	Identifies the method used for protocol identification (PID) in the Call User Data (CUD) field. Because PVCs are not set up using a Call packet, this field is not displayed for encapsulation PVCs. The available methods are as follows: • cisco—Cisco's traditional method was used to set up a single protocol virtual circuit. • ietf—The IETF's standard RFC 1356 method was used to set up a single protocol virtual circuit. • snap—The IETF's Subnetwork Access Protocol (SNAP) method for IP encapsulation was used. • multi—the IETF's multiprotocol encapsulation method was used.
Data PID	Identifies the method used for PID when sending datagrams. The available methods are as follows: • none—The virtual circuit is a single-protocol virtual circuit; no PID is used. • ietf—The IETF's standard RFC 1356 method for identifying the protocol is used. • snap—The IETF's SNAP method for identifying IP datagrams is used.

Locally Switched X.25 Traffic: Example

The following is sample output of the **show x25 vc** command used on a virtual circuit carrying locally switched X.25 traffic:

```
Router# show x25 vc

PVC 1, State: D1, Interface: Serial2
  Started 0:01:26, last input never, output never
  PVC <--> Serial1 PVC 1, connected
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 0 PR: 0 ACK: 0 Remote PR: 0 RCNT: 0 RNR: FALSE
  P/D state timeouts: 0 Timer (secs): 0
  data bytes 0/0 packets 0/0 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0

SVC 5, State: D1, Interface: Serial2
  Started 0:00:16, last input 0:00:15, output 0:00:15
  Connects 170093 <--> 170090 from Serial1 VC 5
  Window size input: 2, output: 2
```

```
  Packet size input: 128, output: 128
  PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
  P/D state timeouts: 0 Timer (secs): 0
  data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Table 94 describes the connection fields for virtual circuits carrying locally switched X.25 traffic.

Table 94 show x25 vc Local Traffic Field Descriptions

Field	Description
PVC <-->	Indicates a switched connection between two PVCs.
Serial1 PVC 1	Identifies the other half of a local PVC connection.
connected	Identifies connection status for a switched connection between two PVCs. See Table 97 for PVC status messages.
170093	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed. If the source host is a CMNS host, its MAC address is also displayed.
170090	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed. If the destination host is a CMNS host, its MAC address is also displayed.
from Serial1	Indicates the direction of the call and the connecting interface.
VC 5	Identifies the circuit type and LCN for the connecting interface. VC indicates an SVC, and PVC indicates a PVC. If the connecting host is a CMNS host, its MAC address is also displayed.

X.25 Traffic Locally Switched Between PVCs and SVCs: Example

The following is sample output of the **show x25 vc** command used on a virtual circuit carrying locally switched PVC-to-SVC X.25 traffic:

```
Router# show x25 vc

PVC 5,  State: D1,  Interface: Serial0
  Started 4d21h, last input 00:00:14, output 00:00:14
  Connects 101600 <--> 201700 from Serial2 VC 700
  D-bit permitted
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 5  PR: 5  ACK: 4  Remote PR: 5  RCNT: 1  RNR: no
  P/D state timeouts: 0  timer (secs): 0
  data bytes 1000/1000 packets 10/10 Resets 1/0 RNRs 0/0 REJs 0/0 INTs 0/0

SVC 700,  State: D1,  Interface: Serial2
  Started 00:00:16, last input 00:00:16, output 00:00:16
  Connects 101600 <--> 201700 from Serial0 PVC 5
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 5  PR: 5  ACK: 5  Remote PR: 4  RCNT: 0  RNR: no
  P/D state timeouts: 0  timer (secs): 103
  data bytes 500/500 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Table 95 describes the connection fields for virtual circuits carrying locally switched X.25 traffic between PVCs and SVCs.

Table 95 show x25 vc Locally Switched PVC-to-SVC Traffic Field Descriptions

Field	Description
101600	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed. If the source host is a CMNS host, its MAC address is also displayed.
201700	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed. If the destination host is a CMNS host, its MAC address is also displayed.
from Serial2	Indicates the direction of the call and the connecting interface.
VC 700	Identifies the circuit type and LCN for the connecting interface. VC indicates an SVC and PVC indicates a PVC. If the remote host is a CMNS host, its MAC address is also displayed.

Remotely Switched X.25 Traffic: Example

The following is sample output from the **show x25 vc** command used on a virtual circuit carrying remotely switched X.25 traffic:

```
Router# show x25 vc

PVC 2, State: D1, Interface: Serial2
 Started 0:01:25, last input never, output never
 PVC <--> [172.20.165.92] Serial2/0 PVC 1 connected
 XOT between 172.20.165.95, 1998 and 172.20.165.92, 27801
 Window size input: 2, output: 2
 Packet size input: 128, output: 128
 PS: 0 PR: 0 ACK: 0 Remote PR: 0 RCNT: 0 RNR: FALSE
 P/D state timeouts: 0 Timer (secs): 0 Reassembly (bytes): 0
 Held Fragments/Packets: 0/0
 data bytes 0/0 packets 0/0 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0

SVC 6, State: D1, Interface: Serial2
 Started 0:00:04, last input 0:00:04, output 0:00:04
 Connects 170093 <--> 170090 from
 XOT between 172.20.165.91, 1998 and 172.20.165.92, 27896
 Window size input: 2, output: 2
 Packet size input: 128, output: 128
 PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
 P/D state timeouts: 0 Timer (secs): 0 Reassembly (bytes): 0
 Held Fragments/Packets: 0/0
 data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Table 96 describes the connection fields for virtual circuits carrying remotely switched X.25 traffic.

Table 96 show x25 vc Remote X.25 Traffic Field Descriptions

Field	Description
PVC	Flags PVC information.
[172.20.165.92]	Indicates the IP address of the router remotely connecting the PVC.
Serial 2/0 PVC 1	Identifies the remote interface and PVC number.
connected	Identifies connection status for a switched connection between two PVCs. See Table 97 for PVC status messages.

Table 96 show x25 vc Remote X.25 Traffic Field Descriptions (continued)

Field	Description
170093	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed.
170090	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed.
from	Indicates the direction of the call.
XOT between...	Identifies the IP addresses and port numbers of the X.25-over-TCP (XOT) connection.

Table 97 lists the PVC states that can be reported. These states are also reported by the **debug x25** command in PVC-SETUP packets (for remote PVCs only). Some states apply only to remotely switched PVCs.

Table 97 X.25 PVC Status Messages

Status Message	Description
awaiting PVC-SETUP reply	A remote PVC has initiated an XOT TCP connection and is waiting for a reply to the setup message.
can't support flow control values	The window sizes or packet sizes of the PVC cannot be supported by one of its two interfaces.
connected	The PVC is up.
dest. disconnected	The other end has disconnected the PVC.
dest interface is not up	The target interface's X.25 service is down.
dest PVC config mismatch	The targeted PVC is already connected.
mismatched flow control values	The configured flow control values do not match.
no such dest. interface	The remote destination interface was reported to be in error by the remote router.
no such dest. PVC	The targeted PVC does not exist.
non-X.25 dest. interface	The target interface is not configured for X.25.
PVC/TCP connect timed out	A remote PVC XOT TCP connection attempt timed out.
PVC/TCP connection refused	A remote PVC XOT TCP connection was tried and refused.
PVC/TCP routing error	A remote PVC XOT TCP connection routing error was reported.
trying to connect via TCP	A remote PVC XOT TCP connection is established and is in the process of connecting.
waiting to connect	The PVC is waiting to be processed for connecting.

show x25 xot

To display information for all X.25 over TCP (XOT) virtual circuits that match a given criterion, use the **show x25 xot** command in privileged EXEC mode.

show x25 xot [**local** *ip-address* [**port** *port*]] [**remote** *ip-address* [**port** *port*] | **access-group** [*access-group-number*]]

Syntax Description

local *ip-address* [**port** *port*]	(Optional) Local IP address and optional port number.
remote *ip-address* [**port** *port*]	(Optional) Remote IP address and optional port number.
access-group	(Optional) Displays configuration information about XOT access groups.
access-group-number	(Optional) Displays configuration information about a specific XOT access group.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(8)T	Access group 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.

Examples

The following **show x25 xot** sample output displays information about all XOT virtual circuits:

```
Router# show x25 xot

SVC 11,  State: D1,  Interface: [10.2.2.2,1998/10.2.2.1,11002]
  Started 00:00:08, last input 00:00:08, output 00:00:08

  Line: 0   con 0    Location:  Host: 5678
  111 connected to 5678 PAD <--> XOT 2.2.2.2,1998

  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 2  PR: 3  ACK: 3  Remote PR: 2  RCNT: 0  RNR: no
  P/D state timeouts: 0  timer (secs): 0
  data bytes 54/18 packets 2/3 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0\
```

The following example shows sample output for the **show x25 xot** command with the **access-group** keyword:

```
Router# show x25 xot access-group

 xot access-group 1 using built-in default configuration
 xot access-group 10 using x.25 profile ocean
 xot access-group 55 using x.25 profile river
```

Related Commands

Command	Description
show x25 interface	Displays information about VCs that use an X.25 interface and, optionally, about a specified VC.
show x25 services	Displays information pertaining to the X.25 services.

show x28 hunt-group

To display the members and status of each member in an X.28 hunt group, use the **show x28 hunt-group** command in user EXEC or privileged EXEC mode.

show x28 hunt-group [*group-num*]

Syntax Description

group-num	(Optional) Identification number of a particular hunt group.

Command Default

The members of all X.28 hunt groups in the router are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)YN	This command was introduced.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Examples

The following example displays the configuration of four hunt ("rotary") groups and the current status of their member lines:

```
Router# show x28 hunt-group

   ID  Type    HG-Address TTy      Address Uses   status
   ================================================================================
   1   RRA         23456      97      34567   2       INUSE
                              98      12345   0      NXTUSE
                              100     -       0       INUSEO
                              102     456789  0        IDLE
   2    QBR,FIF    -          99       -      0       UNAVL
   3   QUE,FIF     -          101     -       0      NXTUSE
   4   FIF         56789      103     67890   0       UNAVL
                              104     789012  0       UNAVL
```

Table 98 show x28 hunt-group Field Descriptions

Field	Description
ID	The identification number of the hunt group.
Type	The line-selection mechanism used within the group: • **FIF** (First Idle First): Lines are searched in increasing order of their line (absolute) number, and the first idle line found is given the incoming call. • **RRA** (Round-Robin): The incoming call is given to the line whose line number is the next highest from the line that received the last call. • **QUE** (Queued): If all lines in the group are busy when a call request arrives, that call is queued and given to the first line that frees up. (Not implementable with Multi-PAD X.25 addressing.) • **QBR** (Queued By Role): Same as "Queued," except that calls belonging to priority users are placed at the head of the queue. (Not implementable with Multi-PAD X.25 addressing.)
HG-Address	X.28 address assigned to the hunt group.
TTy	Absolute number of the line.
Address	X.121 address assigned to that line.
Uses	How many calls have been placed on that line.
status	Current status of the line: • **IDLE**: available • **NXTUSE**: idle and next to be used • **INUSE**: busy in a PAD call • **INUSEO**: busy in a non-PAD call • **UNAVL**: unavailable (either because of inactive modem control signals or because PAD transport is unavailable)

show x29 access-lists

To display X.29 access lists, use the **show x29 access-lists** command in user EXEC or privileged EXEC mode.

show x29 access-lists [*access-list-number*]

Syntax Description

access-list-number	(Optional) Standard x29 access list number. The range is from 0 to 500.

Command Default

If no argument is specified, information for all X.29 access lists is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced in a release earlier than Cisco IOS Release 12.0.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show x29 access-lists** command:

```
Router# show x29 access-lists

X29 access list 10
    permit 192.0.2.0
X29 access list 20
    deny 192.0.2.255
X29 access list 50
    permit 192.0.2.10
```

Table 99 describes the significant fields shown in the display.

Table 99 show x29 access-lists Field Descriptions

Field	Description
X29 access list	Displays the access list number which is configured to be allowed or denied access.

Table 99 show x29 access-lists Field Descriptions (continued)

Field	Description
permit	Displays the source IP address of the incoming packet which is permitted to have access to the protocol translator.
deny	Displays the source IP address of the incoming packet which is configured to deny access and clear call requests immediately.

Related Commands

Command	Description
x29 access-list	Limits access to the access server from certain X.25 hosts.

show xconnect

To display information about xconnect attachment circuits and pseudowires, use the **show xconnect** command in user EXEC or privileged EXEC mode.

show xconnect {{**all** | **interface** *type number*} [**detail**] | **peer** *ip-address* {**all** | **vcid** *vcid-value*} [**detail**] | **pwmib** [**peer** *ip-address vcid-value*]}

Cisco IOS SR and S Trains

show xconnect {{**all** | **interface** *type number* | **memory** | **rib**} [**detail**] [**checkpoint**] | **peer** *ip-address* {**all** | **vcid** *vcid-value*} [**detail**] | **pwmib** [**peer** *ip-address vcid-value*]}

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

show xconnect {**all** | **peer** *ip-address* {**all** | **vcid** *vcid-value*} | **pwmib** [**peer** *ip-address vcid-value*]} [**detail**]

Syntax Description

all	Displays information about all xconnect attachment circuits and pseudowires.
interface	Displays information about xconnect attachment circuits and pseudowires on the specified interface.
type	Interface type. For more information, use the question mark (?) online help function. Valid values for the *type* argument are as follows: • **atm** *number*—Displays xconnect information for a specific ATM interface or subinterface. • **atm** *number* **vp** *vpi-value*—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command will not display information about virtual circuit (VC) xconnects using the specified VPI. • **atm** *number* **vc** *vpi-value*/*vci-value*—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination. • **ethernet** *number*—Displays port-mode xconnect information for a specific Ethernet interface or subinterface. • **fastethernet** *number*—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface. • **serial** *number*—Displays xconnect information for a specific serial interface. • **serial** *number dlci-number*—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and pseudowires.

checkpoint	(Optional) Displays the autodiscovered pseudowire information that is checkpointed to the standby Route Processor (RP).
peer	Displays information about xconnect attachment circuits and pseudowires associated with the specified peer.
ip-address	The IP address of the peer.
all	Displays all xconnect information associated with the specified peer IP address.
vcid	Displays xconnect information associated with the specified peer IP address and the specified VC ID.
vcid-value	VC ID value.
pwmib	Displays information about the pseudowire Management Information Base (MIB).
memory	Displays information about the xconnect memory usage.
rib	Displays information about the pseudowire Routing Information Base (RIB).

Command Modes

User EXEC (>)
Privileged EXEC (#)

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 modified. The **rib** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **pwmib** keyword was added.
12.2(33)SRC	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SRC. The **memory** keyword was added.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. The output of the **show xconnect rib** command and the **show xconnect rib detail** command was modified to support dynamic pseudowire switching on Autonomous System Boundary Routers (ASRBs). The **checkpoint** keyword was added.

Usage Guidelines

The **show xconnect** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and pseudowires.

You can use the **show xconnect** command output to help determine the appropriate steps required to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the “Related Commands” table.

Examples

The following example shows the **show xconnect all** command output in the brief (default) display format:

```
Router# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No Hardware
XC ST     Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
IA sec ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.3:2231              DN
UP     ac   Se4/0(HDLC)                  UP mpls 10.55.55.2:4000              UP
UP     ac   Se6/0:500(FR DLCI)           UP l2tp 10.55.55.2:5000              UP
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
UP pri ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.2:5225              UP
IA sec ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.3:5226              DN
IA pri ac   Et1/0.2:100(Eth VLAN)        UP ac   Et2/0.2:100(Eth VLAN)        UP
UP sec ac   Et1/0.2:100(Eth VLAN)        UP mpls 10.55.55.3:1101              UP
UP     ac   Se6/0:150(FR DLCI)           UP ac   Se8/0:150(FR DLCI)           UP
```

The following example shows the **show xconnect all** command output in the detailed display format:

```
Router# show xconnect all detail

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, SB=Standby, RV=Recovering, NH=No HardwareXC
ST     Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000              UP
            Interworking: ip                      Local VC label 16
                                                  Remote VC label 16
                                                  pw-class: mpls-ip
UP     ac   Se7/0(PPP)                   UP mpls 10.55.55.2:2175              UP
            Interworking: ip                      Local VC label 22
                                                  Remote VC label 17
                                                  pw-class: mpls-ip
UP pri ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.2:2230              UP
            Interworking: ip                      Local VC label 21
                                                  Remote VC label 18

pw-class: mpls-ip
IA sec ac   Se6/0:230(FR DLCI)           UP mpls 10.55.55.3:2231              DN
            Interworking: ip                      Local VC label unassigned
                                                  Remote VC label 19
                                                  pw-class: mpls-ip
SB ac   Se4/0:100(FR DLCI)           UP mpls 10.55.55.2:4000              SB
            Interworking: none                    Local VC label 18
                                                  Remote VC label 19
                                                  pw-class: mpls
UP     ac   Se6/0:500(FR DLCI)           UP l2tp 10.55.55.2:5000              UP
            Interworking: none                    Session ID: 34183
                                                  Tunnel ID: 62083
                                                  Peer name: pe-iou2
                                                  Protocol State: UP
                                                  Remote Circuit State: UP
                                                  pw-class: l2tp
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
            Interworking: ip                      Local VC label 17
                                                  Remote VC label 20
                                                  pw-class: mpls-ip
UP pri ac   Se6/0:225(FR DLCI)           UP mpls 10.55.55.2:5225              UP
            Interworking: none                    Local VC label 19
                                                  Remote VC label 21
```

```
                                                pw-class: mpls
IA sec ac   Se6/0:225(FR DLCI)          UP mpls 10.55.55.3:5226              DN
            Interworking: none                  Local VC label unassigned
                                                Remote VC label 22
                                                pw-class: mpls
IA pri ac   Et1/0.2:100(Eth VLAN)       UP ac   Et2/0.2:100(Eth VLAN)       UP
            Interworking: none                  Interworking: none
UP sec ac   Et1/0.2:100(Eth VLAN)       UP mpls 10.55.55.3:1101              UP
            Interworking: none                  Local VC label 23
                                                Remote VC label 17
                                                pw-class: mpls
UP     ac   Se6/0:150(FR DLCI)          UP ac   Se8/0:150(FR DLCI)          UP
            Interworking: none                  Interworking: none
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Brief Display Format

The following is sample output from the **show xconnect** command in the brief (default) display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2                        S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)          UP mpls 10.76.1.1:2001              UP
UP     ac   Bu254:2002(DOCSIS)          UP mpls 10.76.1.1:2002              UP
UP     ac   Bu254:2004(DOCSIS)          UP mpls 10.76.1.1:2004              UP
DN     ac   Bu254:22(DOCSIS)            UP mpls 101.1.0.2:22                DN
```

Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Detailed Display Format

The following is sample output from the **show xconnect** command in the detailed display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all detail

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware

XC ST  Segment 1                        S1 Segment 2                        S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)          UP mpls 10.76.1.1:2001              UP
            Interworking: ethernet              Local VC label 40
                                                Remote VC label 110
                                                pw-class:
UP     ac   Bu254:2002(DOCSIS)          UP mpls 10.76.1.1:2002              UP
            Interworking: ethernet              Local VC label 41
                                                Remote VC label 88
                                                pw-class:
UP     ac   Bu254:2004(DOCSIS)          UP mpls 10.76.1.1:2004              UP
            Interworking: ethernet              Local VC label 42
                                                Remote VC label 111
                                                pw-class:
```

```
DN      ac    Bu254:22(DOCSIS)             UP mpls 101.1.0.2:22                DN
              Interworking: ethernet               Local VC label 39
                                                   Remote VC label unassigned
                                                   pw-class:
```

Table 100 describes the significant fields shown in the displays.

Table 100 show xconnect all Field Descriptions

Field	Description
XC ST	State of the xconnect attachment circuit or pseudowire. The valid states are: • DN—The xconnect attachment circuit or pseudowire is down. Either segment 1, segment 2, or both segments are down. • IA—The xconnect attachment circuit or pseudowire is inactive. This state is valid only when pseudowire redundancy is configured. • NH—One or both segments of this xconnect no longer have the required hardware resources available to the system. • UP—The xconnect attachment circuit or pseudowire is up. Both segment 1 and segment 2 must be up for the xconnect to be up.
Segment1 or Segment2	Information about the type of xconnect, the interface type, and the IP address the segment is using. The types of xconnects are as follows: • ac—Attachment circuit • l2tp—Layer 2 Tunnel Protocol • mpls—Multiprotocol Label Switching • pri ac—Primary attachment circuit • sec ac—Secondary attachment circuit
S1 or S2	State of the segment. The valid states are: • AD—The segment is administratively down. • DN—The segment is down. • HS—The segment is in hot standby mode. • RV—The segment is recovering from a graceful restart. • SB—The segment is in a standby state. • UP—The segment is up.

The additional fields displayed in the detailed output are self-explanatory.

VPLS Autodiscovery Feature Example

For the VPLS Autodiscovery feature, issuing the **show xconnect** command with the **rib** keyword provides RIB details, as shown in the following example:

```
Router# show xconnect rib

Local Router ID: 10.9.9.9

Legend: O=Origin, P=Provisioned, TID=Target ID, B=BGP, Y=Yes, N=No
O P  VPLS/VPWS-ID         TID        Next-Hop        Route-Target
-+-+--------------------+-----------+--------------+--------------------
B Y 10:123                192.0.2.0    192.0.2.5     10:123
```

```
B N 10:123                192.0.2.1    192.0.2.6     10:123
B Y 10.100.100.100:1234   192.0.2.3    192.0.2.7     10.111.111.111:12345
                                       192.0.2.8     10.8.8.8:345
                                       192.0.2.9
B Y 192.0.3.1:1234        192.0.2.4 10.1.1.1         10.111.111.111:12345
```

Table 101 describes the significant fields shown in the display.

Table 101 show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
O	Origin of the route.
P	Indicates whether the pseudowire has been provisioned using a learned route.
VPLS/WPWS-ID	Virtual Private LAN Service (VPLS) domain. VPLS Autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
TID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

For VPLS Autodiscovery, issuing the **show xconnect** command with the **rib** and **detail** keywords provides more information about the routing information base, as shown in the following example:

```
Router# show xconnect rib detail

Local Router ID: 10.9.9.9

VPLS-ID 10:123, TID 10.7.7.7
  Next-Hop: 10.7.7.7
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:10
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10:123, TID 10.7.7.8
  Next-Hop: 10.7.7.8
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:11
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: No
VPLS-ID 10.100.100.100:1234, TID 0.0.0.2
  Next-Hop: 10.2.2.2, 10.3.3.3, 10.4.4.4
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345, 10.8.8.8:345
  Incoming RD: 10:12
  Forwarder: vfi VPLS2
```

```
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10.100.100.100:1234, TID 10.13.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345
  Incoming RD: 10:13
  Forwarder: vfi VPLS2
  Origin: BGP
  Provisioned: Yes
```

Table 102 describes the significant fields shown in the display.

Table 102 show xconnect rib detail Field Descriptions

Field	Description
Hello-Source	Source IP address used when Label Distribution Protocol (LDP) hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Incoming RD	Route distinguisher for the autodiscovered pseudowire.
Forwarder	VFI to which the autodiscovered pseudowire is attached.

L2VPN VPLS Inter-AS Option B Examples

The following is sample output from the **show xconnect rib** command when used in an L2VPN VPLS Inter-AS Option B configuration:

```
Router# show xconnect rib

Local Router ID: 10.9.9.9

+- Origin of entry  (i=iBGP/e=eBGP)
| +- Provisioned    (Yes/No)?
| | +- Stale entry  (Yes/No)?
| | |
v v v
O P S        VPLS-ID         Target ID       Next-Hop        Route-Target
-+-+-+------+---------------+---------------+---------------+-------------
i Y N        1:1             10.11.11.11     10.11.11.11     1:1
i Y N        1:1             10.12.12.12     10.12.12.12     1:1
```

Table 103 describes the significant fields shown in the display.

Table 103 show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
Origin of entry	Origin of the entry. The origin can be “i” for internal BGP or “e” for external BGP.
Provisioned	Indicates whether the pseudowire has been provisioned using a learned route; Yes or No.
Stale entry	Stale entry; Yes or No.

Table 103 show xconnect rib Field Descriptions (continued)

Field	Description
VPLS-ID	Virtual Private LAN Service (VPLS) domain. VPLS Autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
Target ID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

The following is sample output from the **show xconnect rib detail** command when used in an ASBR configuration. On an ASBR, the **show xconnect rib detail** command displays the Layer 2 VPN BGP network layer reachability information (NLRI) received from the BGP peers. The display also shows the signaling messages received from the targeted Label Distribution Protocol (LDP) sessions for a given target attachment individual identifier (TAII).

```
Router# show xconnect rib detail

Local Router ID: 10.1.1.3

VPLS-ID: 1:1, Target ID: 10.1.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.1.1.3
  Route-Target: 2:2
  Incoming RD: 10.0.0.0:1
  Forwarder:
  Origin: BGP
  Provisioned: Yes
  SAII: 10.0.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1001 ***
  SAII: 10.1.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1002 ***
```

After the passive TPE router receives the BGP information (and before the passive TPE router receives the LDP label), the peer information will be displayed in the output of the **show xconnect rib** command. The peer information will not be displayed in the **show mpls l2transport vc** command because the VFI AToM xconnect has not yet been provisioned.

Therefore, for passive TPEs, the entry “Passive : Yes” is added to the output from the **show xconnect rib detail** command. In addition, the entry “Provisioned: Yes” is displayed after the neighbor xconnect is successfully created (without any retry attempts).

In the sample output, the two lines beginning with “SAII” show that this ASBR is stitching two provider PE routers (10.0.0.1 and 10.1.0.1) to the TAII 10.1.1.1.

Table 104 describes the significant fields shown in the display.

Table 104 show xconnect rib detail (for the ASBR) Field Descriptions

Field	Description
VPLS-ID	VPLS identifier.
Target ID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.

Table 104 show xconnect rib detail (for the ASBR) Field Descriptions (continued)

Field	Description
Hello-Source	Source IP address used when LDP hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.
Incoming RD	Route distinguisher for the autodiscovered pseudowire.
Forwarder	VFI to which the autodiscovered pseudowire is attached.
Origin	Origin of the entry.
Provisioned	Indicates whether the neighbor xconnect was successfully created (without any retry attempts).
SAII	Source attachment individual identifier.

The following is sample output from the **show xconnect rib checkpoint** command. Autodiscovered pseudowire information is checkpointed to the standby Route Processor (RP). The **show xconnect rib checkpoint** command displays that pseudowire information.

```
Router# show xconnect rib checkpoint

Xconnect RIB Active RP:
  Checkpointing   : Allowed
  Checkpoing epoch: 1
  ISSU Client id: 2102, Session id: 82, Compatible with peer

  Add entries send ok     :          0
  Add entries send fail   :          0
  Delete entries send ok  :          0
  Delete entries send fail:          0

  +- Checkpointed to standby (Y/N)?
  | +- Origin of entry (i=iBGP/e=eBGP)
  | |
  v v
  C O       VPLS-ID        Target ID         Next-Hop      Route-Target
  -+-+--------------------+---------------+---------------+----------------
  N e 1:1                   10.1.1.2         10.1.1.2         2:2
  N e 1:1                   10.1.1.1         10.1.1.3         2:2
```

Table 105 describes the significant fields shown in the display.

Table 105 show xconnect rib checkpoint Field Descriptions

Field	Description
Checkpointing	Indicates whether checkpointing is allowed.
Checkpointing epoch	Checkpointing epoch number.
Checkpointed to standby	Indicates whether the autodiscovered pseudowire information is checkpointed to the standby RP.
Origin of entry	Origin of the entry; “i” for internal BGP or “e” for external BGP.
VPLS-ID	VPLS identifier.

Table 105 show xconnect rib checkpoint Field Descriptions (continued)

Field	Description
Target ID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the RD and VPN ID.

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
show atm vc	Displays all ATM PVCs and SVCs and traffic information.
show atm vp	Displays the statistics for all VPs on an interface or for a specific VP.
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

shutdown (FR-ATM)

To shut down a Frame Relay-ATM Network Interworking (FRF.5) connection or a Frame Relay-ATM Service Interworking (FRF.8) connection, use the **shutdown** command in FRF.5 or FRF.8 connect configuration mode. To disable disconnection, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

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

An FRF.5 or FRF.8 connection must be manually shut down once the interworking connection is created by use of the **shutdown** command.

Examples

FRF.5 Shutdown: Example

The following example shows how to shut down an FRF.5 connection:

```
Router(config)# connect network-2 interface serial0/1 16 atm3/0 0/32 network-interworking
.
.
.
Router(config-frf5)# shutdown
```

FRF.8 Shutdown: Example

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

```
Router(config)# connect serial0 100 atm3/0 1/35 service-interworking
.
.
.
Router(config-frf8)# shutdown
```

Related Commands

Command	Description
connect (FRF.5)	Connects a Frame Relay DLCI or VC group to an ATM PVC.

smds address

To specify the Switched Multimegabit Data Service (SMDS) individual address for a particular interface, use the **smds address** command in interface configuration mode. To remove the address from the configuration file, use the **no** form of this command.

smds address *smds-address*

no smds address *smds-address*

Syntax Description

smds-address	Individual address provided by the SMDS service provider. It is protocol independent.

Defaults

No address is specified.

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

All addresses for SMDS service are assigned by the service provider, and can be assigned to individuals and groups.

Addresses are entered in the Cisco SMDS configuration software using an E prefix for *multicast* addresses and a C prefix for *unicast* addresses. Cisco IOS software expects the addresses to be entered in E.164 format, which is 64 bits. The first 4 bits are the address type, and the remaining 60 bits are the address. If the first 4 bits are 1100 (0xC), the address is a unicast SMDS address, which is the address of an individual SMDS host. If the first 4 bits are 1110 (0xE), the address is a multicast SMDS address, which is used to broadcast a packet to multiple end points. The 60 bits of the address are in binary-coded decimal (BCD) format. Each 4 bits of the address field presents a single telephone number digit, allowing for up to 15 digits. At a minimum, you must specify at least 11 digits (44 bits). Unused bits at the end of this field are filled with ones.

Note If bridging is enabled on any interface, the SMDS address is erased and must be reentered.

Examples

The following example specifies an individual address in Ethernet-style notation:

```
interface serial 0
 smds address c141.5797.1313.FFFF
```

smds dxi

To enable the Data Exchange Interface (DXI) version 3.2 support, use the **smds dxi** command in interface configuration mode. To disable the DXI 3.2 support, use the **no** form of this command.

smds dxi

no smds dxi

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

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

Adding this command to the configuration enables the DXI version 3.2 mechanism and encapsulates SMDS packets in a DXI frame before they are transmitted. DXI 3.2 adds an additional 4 bytes to the SMDS packet header to communicate with the SMDS data service unit (SDSU). These bytes specify the frame type. The interface expects all packets to arrive with DXI encapsulation.

The DXI 3.2 support also includes the heartbeat process as specified in the SIG-TS-001/1991 standard, revision 3.2. The heartbeat (active process) is enabled when both DXI and keepalives are enabled on the interface. The echo (passive process) is enabled when DXI is enabled on the interface. The heartbeat mechanism automatically generates a heartbeat poll frame every 10 seconds. This default value can be changed with the **keepalive** (LMI) command.

Fast switching of DXI frames is supported, but Interim Local Management Interface (ILMI) is not.

Note If you are running serial lines back-to-back, disable keepalive on SMDS interfaces. Otherwise, DXI declares the link down.

Note Switching in or out of DXI mode causes the IP cache to be cleared. This clearing process is necessary to remove all cached IP entries for the serial line being used. Stale entries must be removed to allow the new MAC header with or without DXI framing to be installed in the cache. This clearing process is not frequently done and is not considered to be a major performance penalty.

Examples

The following example enables DXI 3.2 on interface HSSI 0:

```
interface hssi 0
 encapsulation smds
 smds dxi
 smds address C120.1111.2222.FFFF
 ip address 172.20.1.30 255.255.255.0
 smds multicast ip E180.0999.9999
 smds enable-arp
```

Related Commands

Command	Description
keepalive (**LMI**)	Enables the LMI mechanism for serial lines using Frame Relay encapsulation.

smds enable-arp

To enable dynamic Address Resolution Protocol (ARP), use the **smds enable-arp** interface configuration command. The multicast address for ARP must be set before this command is issued. To disable the interface once ARP has been enabled, use the **no** form of this command.

smds enable-arp

no smds enable-arp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

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.

Examples

The following example enables the dynamic ARP routing table:

```
interface serial 0
 ip address 172.20.1.30 255.255.255.0
 smds multicast IP E180.0999.9999.2222
 smds enable-arp
```

Related Commands

Command	Description
arp	Enables ARP entries for static routing over the SMDS network.

smds glean

To enable dynamic address mapping for Internet Packet Exchange (IPX) over Switched Multimegabit Data Service (SMDS), use the **smds glean** interface configuration command. To disable dynamic address mapping for IPX over SMDS, use the **no** form of this command.

smds glean *protocol* [*timeout-value*] [**broadcast**]

no smds glean *protocol*

Syntax Description

protocol	Protocol type. Only IPX is supported.
timeout-value	(Optional) Time to live (TTL) value. Value can be from 1 to 65535 minutes. The default is 5 minutes. This value indicates how long a gleaned dynamic map is stored in the SMDS map table.
broadcast	(Optional) Marks the gleaned protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1	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 **smds glean** command uses incoming packets to dynamically map SMDS addresses to higher-level protocol addresses. Therefore the need for static map configuration for the IPX protocol is optional rather than mandatory. However, any static map configuration overrides the dynamic maps.

If a map is gleaned and it already exists as a dynamic map, the timer for the dynamic map is reset to the default value or the user-specified value.

Examples

The following example enables dynamic address mapping for IPX on interface serial 0 and sets the time to live (TTL) to 14 minutes:

```
interface serial 0
 encapsulation smds
 smds address c141.5797.1313.FFFF
 smds multicast ipx e1800.0999.9999.FFFF
 smds glean ipx 14
```

smds multicast

To assign a multicast Switched Multimegabit Data Service (SMDS) E.164 address to a higher-level protocol, use the **smds multicast** command in interface configuration mode. To remove an assigned multicast address, use the **no** form of this command.

smds multicast *protocol smds-address*

no smds multicast *protocol smds-address*

Syntax Description

protocol	Protocol type. See Table 106 for a list of supported protocols and their keywords.
smds-address	SMDS address. Because SMDS does not incorporate broadcast addressing, a group address for a particular protocol must be defined to serve the broadcast function.

Defaults

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	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

When configuring DECnet, you must enter all four DEC keywords (**decnet**, **decnet_router-L1**, **decnet_router-L2**, and **decnet_node**) in the configuration.

Table 106 lists the high-level protocols supported by the **smds multicast** command.

Table 106 smds multicast Supported Protocols

Keyword	Protocol
aarp	AppleTalk Address Resolution Protocol
appletalk	AppleTalk
arp	Address Resolution Protocol
bridge	Transparent bridging
clns	International Organization for Standardization (ISO) Connectionless Network Service (CLNS)
clns_es	Multicast address for all CLNS end systems
clns_is	Multicast address for all CLNS intermediate systems
decnet	DECnet
decnet_node	DECnet multicast address for all end systems
decnet_router-L1	DECnet multicast address for all Level 1 (intra-area) routers
decnet_router-L2	DECnet multicast address for all Level 2 (interarea) routers
ip	Internet Protocol (IP)
ipx	Novell IPX

For IP, the IP NETwork and MASK fields are no longer required. The Cisco IOS software accepts these arguments, but ignores the values. These were required commands for the previous multiple logical IP subnetworks configuration. The software continues to accept the arguments to allow for backward compatibility, but ignores the contents.

Examples

The following example maps the IP broadcast address to the SMDS group address E180.0999.9999:

```
interface serial 0
 smds multicast IP E180.0999.9999.FFFF
```

smds multicast arp

To map the Switched Multimegabit Data Service (SMDS) address to a multicast address, use the **smds multicast arp** interface configuration command. To disable this feature, use the **no** form of this command.

smds multicast arp *smds-address* [*ip-address mask*]

no smds multicast arp *smds-address* [*ip-address mask*]

Syntax Description

smds-address	SMDS address in E.164 format.
ip-address	(Optional) IP address.
mask	(Optional) Subnet mask for the IP address.

Defaults

No mapping is defined.

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

This command is used only when an Address Resolution Protocol (ARP) server is present on a network. When broadcast ARPs are sent, SMDS first attempts to send the packet to all multicast ARP SMDS addresses. If none exist in the configuration, broadcast ARPs are sent to all multicast IP SMDS multicast addresses. If the optional ARP multicast address is missing, each entered IP multicast command is used for broadcasting.

Examples

The following example configures broadcast ARP messages:

```
interface serial 0
 smds multicast arp E180.0999.9999.2222
```

Related Commands

Command	Description
smds multicast ip	Maps an SMDS group address to a secondary IP address.

smds multicast bridge

To enable spanning-tree updates, use the **smds multicast bridge** interface configuration command. To disable this function, use the **no** form of this command.

smds multicast bridge *smds-address*

no smds multicast bridge *smds-address*

Syntax Description

smds-address	SMDS multicast address in E.164 format.

Defaults

No multicast SMDS address is defined. Spanning tree updates are disabled for transparent bridging across SMDS networks.

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

To allow transparent bridging of packets across serial and High-Speed Serial Interface (HSSI) interfaces in an SMDS network, the SMDS interface must be added to an active bridge group. Also, standard bridging commands are necessary to enable bridging on an SMDS interface.

When the **smds multicast bridge** command is added to the configuration, broadcast packets are encapsulated with the specified SMDS multicast address configured for bridging. Two broadcast Address Resolution Protocol (ARP) packets are sent to the multicast address. One is sent with a standard (SMDS) ARP encapsulation, while the other is sent with the ARP packet encapsulated in an 802.3 MAC header. The native ARP is sent as a regular ARP broadcast.

Cisco's implementation of IEEE 802.6i transparent bridging for SMDS supports 802.3, 802.5, and FDDI frame formats. The router can accept frames with or without frame check sequence (FCS). Fast-switched transparent bridging is the default and is not configurable. If a packet cannot be fast switched, it is process switched.

In Cisco IOS Release 10.2 software (or earlier), bridging over multiple logical IP subnetworks is not supported. Bridging of IP packets in a multiple logical IP subnetworks environment is unpredictable.

Examples

In the following example, all broadcast bridge packets are sent to the configured SMDS multicast address:

```
interface hssi 0
 encapsulation smds
 smds address C120.1111.2222.FFFF
 ip address 172.16.0.0 255.255.255.0
 smds multicast bridge E180.0999.9999.FFFF
 bridge-group 5
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

smds multicast ip

To map a Switched Multimegabit Data Service (SMDS) group address to a secondary IP address, use the **smds multicast ip** interface configuration command. To remove the address map, use the **no** form of this command.

smds multicast ip *smds-address* [*ip-address mask*]

no smds multicast ip *smds-address* [*ip-address mask*]

Syntax Description

smds-address	SMDS address in E.164 format.
ip-address	(Optional) IP address.
mask	(Optional) Subnet mask for the IP address.

Defaults

The IP address and mask default to the primary address of the interface if they are left out of the configuration.

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

This command allows a single SMDS interface to be treated as multiple logical IP subnetworks. If taking advantage of the multiple logical IP subnetworks support in SMDS, you can use more than one multicast address on the SMDS interface (by entering multiple commands). However, each **smds multicast ip** command entry must be associated with a different IP address on the SMDS interface.

Broadcasts can be sent on the SMDS interface by means of the multicast address. By sending broadcasts in this manner, the router is not required to replicate broadcasts messages to every remote host.

In addition, the higher-level protocols such as Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) can use the multicast capability by sending one update packet or routing packet to the multicast address.

If the optional IP address and mask arguments are not present, the SMDS address and multicast address are associated with the primary IP address of the interface. This association allows the command to be backward compatible with earlier versions of the software.

If an Address Resolution Protocol (ARP) multicast address is missing, each entered IP multicast command is used for broadcasting. The ARP multicast command has the same format as the IP multicast command and is typically used only when an ARP server is present in the network.

Note All routers at the other end of the SMDS cloud must have the multiple logical IP subnetworks capability enabled. If you allocate a different SMDS subinterface for each logical IP subnetwork on the SMDS interface, you do not have to configure secondary IP addresses.

Examples

The following example configures an interface with two subinterfaces to support two different IP subnets with different multicast addresses to each network:

```
interface serial 2/0
 encapsulation smds
 smds address C120.1111.2222.4444

interface serial 2/0.1 multipoint
 smds addr c111.3333.3333.3333
 ip address 2.2.2.1 255.0.0.0
 smds multicast ip e222.2222.2222.2222
 smds enable-arp

interface serial 2/0.2 multipoint
 smds addr c111.2222.3333.3333.3333
 ip address 2.3.3.3 255.0.0.0
 smds multicast ip E180.0999.9999.FFFF
 smds enable-arp
```

Related Commands

Command	Description
smds multicast arp	Maps the SMDS address to a multicast address.

smds static-map

To configure a static map between an individual Switched Multimegabit Data Service (SMDS) address and a higher-level protocol address, use the **smds static-map** command in interface configuration mode. To remove the map, use the **no** form of this command with the appropriate arguments.

smds static-map *protocol protocol-address smds-address* [**broadcast**]

no smds static-map *protocol protocol-address smds-address* [**broadcast**]

Syntax Description

protocol	Higher-level protocol. It can be one of the following values: **appletalk**, **clns**, **decnet**, **ip**, or **ipx**.
protocol-address	Address of the higher-level protocol.
smds-address	SMDS address, to complete the mapping.
broadcast	(Optional) Marks the specified protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.

Defaults

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	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

The **smds static-map** command provides *pseudobroadcasting* by allowing the use of broadcasts on those hosts that cannot support SMDS multicast addresses.

Examples

The following example illustrates how to enable pseudobroadcasting. The router at address C120.4444.9999 will receive a copy of the broadcast request because the broadcast keyword is specified with the **smds static-map** command. The host at address 172.16.1.15 is incapable of receiving multicast packets. The multicasting is simulated with this feature.

```
interface hssi 0
 encapsulation smds
 smds address C120.1111.2222.FFFF
 ip address 172.16.1.30 255.255.255.0
 smds static-map ip 172.16.1.15 C120.4444.9999.FFFF broadcast
 smds enable-arp
```

The following example illustrates how to enable multicasting. In addition to IP and ARP requests to E100.0999.9999, the router at address C120.4444.9999 will also receive a copy of the multicast request. The host at address 172.16.1.15 is incapable of receiving broadcast packets.

```
interface hssi 0
 encapsulation smds
 smds address C120.1111.2222.FFFF
 ip address 172.16.1.30 255.255.255.0
 smds multicast ip E100.0999.999.FFFF
 smds static-map ip 172.16.1.15 C120.4444.9999.FFFF
 smds enable-arp
```

status admin-down disconnect

To configure Layer 2 tunneling (L2TUN) sessions to disconnect upon attachment circuit (AC) shutdown, use the **status admin-down disconnect** command in pseudowire class configuration mode. To disable disconnection of L2TUN sessions upon AC shutdown, use the **no** form of this command.

status admin-down disconnect

no status admin-down disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Layer 2 tunneling sessions do not disconnect upon attachment circuit (AC) shutdown.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

Use the **show l2tp session** command to determine whether the sessions are disconnected.

Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named ether-pw and configure L2TUN sessions to disconnect on AC shutdown.

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# pseudowire-class ether-pw
 Router(config-pw)# status admin-down disconnect
 Router(config-pw)# end
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
show l2tp session	Displays information about L2TP sessions.
show l2tun tunnel	Displays the current state of Layer 2 Tunneling Protocol (L2TP) tunnels and information about configured tunnels, including local and remote hostnames, aggregate packet counts, and control channel information.

tfo auto-discovery blacklist

To configure a blacklist with autodiscovery for WAAS Express, use the **tfo auto-discovery blacklist** command in parameter-map configuration mode. To remove the configuration, use the **no** form of this command.

tfo auto-discovery blacklist {**enable** | **hold-time** *minutes*}

no tfo auto-discovery blacklist {**enable** | **hold-time** *minutes*}

Syntax Description

enable	Enables a blacklist.
hold-time *minutes*	Configures a blacklist hold time, in minutes. The range is 1 to 10080.

Command Default

Blacklist with autodiscovery is not enabled.

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 enable, configure, and integrate a blacklist with autodiscovery and specify the hold time for a blacklist in WAAS Express. Blacklists enable you to get the benefit of WAAS Express if there are devices in your network that discard packets with TCP options.

Autodiscovery allows the WAAS Express device to automatically discover and connect to a new file server when a Common Internet File System (CIFS) request is received. The autodiscovery of peer WAAS Express devices is achieved using TCP options. These TCP options are recognized and understood only by WAAS Express devices and are ignored by non-WAAS Express devices.

Examples

The following example configures autodiscovery by enabling the blacklist and setting the hold time for 100 minutes:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile)# tfo auto-discovery blacklist enable
Router(config-profile)# tfo auto-discovery blacklist hold-time 100
```

Related Commands

Command	Description
cpu-threshold	Sets the CPU threshold limit.
lz entropy	Enables entropy checking to turn on Lempel-Ziv (LZ) compression.
parameter-map type waas	Defines a WAAS Express parameter map.

Command	Description
policy-map type waas	Configures WAAS Express policy map.
tfo optimize	Configures compression for WAAS Express.

tfo optimize

To configure the compression for WAAS Express, use the **tfo optimize** command in parameter-map configuration mode. To remove the compression, use the **no** form of this command.

tfo optimize {**full** | **dre** {**no** | **yes**} {**compression** {**lz** | **none**}}

no tfo optimize [**full** | **dre** {**no** | **yes**} {**compression** {**lz** | **none**}]

Syntax Description

full	Turns on Data Redundancy Elimination (DRE) and compression.
dre	Enables DRE.
no	Turns off DRE.
yes	Turns on DRE.
compression	Turns on compression.
lz	Turns on Lempel-Ziv (LZ) compression.
none	Turns off LZ compression.

Command Default

Compression is not configured.

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 specify a compression technology to reduce the size of data. WAAS Express uses the following compression technologies to help you transmit data over your WAN:

- DRE
- LZ

These compression technologies reduce the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. By reducing the amount of transferred data, WAAS compression can reduce network utilization and application response times.

LZ compression operates on smaller data streams and keeps limited compression history. DRE operates on significantly larger streams (typically tens to hundreds of bytes or more) and maintains a much larger compression history. Large chunks of redundant data is common in file system operations when files are incrementally changed from one version to another or when certain elements are common to many files, such as file headers and logos.

Examples

The following example turns off the DRE compression and turns on the LZ compression:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile)# tfo optimize dre no compression lz
```

Related Commands

Command	Description
cpu-threshold	Sets the CPU threshold limit.
lz entropy-check	Enables entropy checking to turn on LZ compression.
parameter-map type waas	Defines a WAAS Express parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery blacklist	Configures black list with autodiscovery for WAAS Express.

threshold de

To configure the threshold at which discard eligible (DE)-marked packets will be discarded from switched permanent virtual circuits (PVCs) on the output interface, use the **threshold de** command in Frame Relay congestion management configuration mode. To remove the threshold configuration, use the **no** form of this command.

threshold de *percentage*

no threshold de *percentage*

Syntax Description

percentage	Threshold at which DE-marked packets will be discarded, specified as a percentage of maximum queue size.

Defaults

100%

Command Modes

Frame Relay congestion management 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

You must enable Frame Relay congestion management on the interface before congestion management parameters will be effective. To enable Frame Relay congestion management and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** interface command.

You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **threshold de** command will be effective on switched PVCs.

Examples

The following example shows how to configure a DE threshold of 40% on serial interface 1.

```
interface serial1
 encapsulation frame-relay
 frame-relay congestion-management
  threshold de 40
```

Related Commands

Command	Description
frame-relay congestion-management	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
frame-relay congestion threshold de	Configures the threshold at which DE-marked packets will be discarded from the traffic-shaping queue of a switched PVC.
frame-relay congestion threshold ecn	Configures the threshold at which ECN bits will be set on packets in the traffic-shaping queue of a switched PVC.
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
threshold ecn	Configures the threshold at which ECN bits will be set on packets in switched PVCs on the output interface.

threshold ecn

To configure the threshold at which explicit congestion notification (ECN) bits will be set on packets in switched permanent virtual circuits (PVCs) on the output interface, use the **threshold ecn** command in Frame Relay congestion management configuration mode. To remove the threshold configuration, use the **no** form of this command.

For Frame Relay Switching

threshold ecn {**bc** | **be**} *percentage*

no threshold ecn {**bc** | **be**} *percentage*

For Frame Relay over MPLS

threshold ecn *percentage*

no threshold ecn *percentage*

Syntax Description

bc	Specifies threshold for committed traffic. This keyword is not available for Frame Relay over MPLS.
be	Specifies threshold for excess traffic. This keyword is not available for Frame Relay over MPLS.
percentage	Threshold at which ECN bits will be set on packets, specified as a percentage of maximum queue size. Default is 100 percent.

Defaults

An ECN threshold is not configured.

Command Modes

Frame Relay congestion management configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(26)S	This command was modified for Frame Relay over MPLS.
12.2(27)SXA	This command was integrated into Cisco IOS Release 12.2(27)SXA.
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.

Usage Guidelines

You must enable Frame Relay congestion management on the interface before congestion management parameters will be effective. To enable Frame Relay congestion management and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** interface command.

Frame Relay Switching Guidelines

- You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **threshold ecn** command will be effective on switched PVCs.
- You can configure separate queue thresholds for committed and excess traffic.
- Configure the BECN threshold so that it is greater than or equal to zero and less than or equal to the BECN threshold. Configure the BECN threshold so that it is less than or equal to 100.

Examples

Frame Relay Switching: Example

The following example shows how to configure a Be threshold of 0 and a Bc threshold of 20 percent on serial interface 1.

```
interface serial1
    encapsulation frame-relay
    frame-relay congestion-management
        threshold ecn be 0
        threshold ecn bc 20
```

Frame Relay over MPLS: Example

The following example shows a configuration of interface serial2/1 for a threshold of 50 percent.

```
interface Serial2/1
    bandwidth 50000
    service-policy output output-policy
    frame-relay congestion-management
        threshold ecn 50
```

Related Commands

Command	Description
frame-relay congestion-management	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.

timeout setup

To configure the amount of time allowed to set up a control channel with a remote provider edge (PE) router at the other end of a Layer 2 pseudowire, use the **timeout setup** command in L2TP class configuration mode. To disable the configured value, use the **no** form of this command.

timeout setup *seconds*

no timeout setup *seconds*

Syntax Description

seconds	The number of seconds allowed to set up a Layer 2 control channel. The valid values range from 60 to 6000. The default value is 300 seconds.

Command Default

The default number of seconds allowed to set up a control channel is 300.

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

Use this command to configure the amount of time that can be spent attempting to establish a control channel.

Examples

The following example sets a timeout period of 200 seconds to establish a control channel with a remote peer in Layer 2 pseudowires that have been configured with the L2TP class named l2tp-class:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# timeout setup 200
```

Related Commands

Command	Description
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.

vc-group

To assign multiple Frame Relay data-link connection identifiers (DLCIs) to a virtual circuit (VC) group for Frame Relay-to-ATM Network Interworking (FRF.5), use the **vc-group** command in global configuration mode. To disable the VC group assignments, use the **no** form of this command.

vc-group *group-name*

no vc-group *group-name*

The **vc-group** command requires that you enter the following arguments in VC-group configuration mode to provide a map between Frame Relay DLCIs and Frame Relay-SSCS DLCIs:

fr-interface-name fr-dlci [*fr-sscs-dlci*]

Syntax Description

group-name	A VC group name entered as an 11-character maximum string.

The following syntax description applies to the VC-group entries:

fr-interface-name	Frame Relay interface; for example, serial0/0.
fr-dlci	Frame Relay DLCI number, in the range 16 to 1007.
fr-sscs-dlci	(Optional) Frame Relay SSCS DLCI number, in the range of 16 to 991. Default is 1022.

Defaults

No default behavior or values

Command Modes

Global configuration
VC-group 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 specifies the Frame Relay DLCIs in the VC group and maps them to the Frame Relay-SSCS DLCIs. If the optional FR-SSCS DLCI value is not specified, its value is the same as the Frame Relay DLCI.

Examples

The following example shows how to configure an FRF.5 many-to-one connection. The **vc-group** command maps Frame Relay DLCI 16, 17, 18, and 19 to a VC group named “friends”:

```
Router(config)# vc-group friends
Router(config-vc-group)# serial0 16 16
Router(config-vc-group)# serial0 17 17
Router(config-vc-group)# serial0 18 18
Router(config-vc-group)# serial0 19 19
```

Related Commands

Command	Description
show vc-group	Displays the names of all VC groups.

vpls-id

To assign an identifier to the Virtual Private LAN Service (VPLS) domain, use the **vpls-id** command in L2 VFI configuration mode. To revert to the default VPLS ID, use the **no** form of this command.

vpls-id {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

no vpls-id {*autonomous-system-number*:*nn* | *ip-address*:*nn*}

Syntax Description

autonomous-system-number:*nn*	Specifies a 16-bit autonomous system number and 32-bit arbitrary number. The autonomous system number need not match the local autonomous system number.
ip-address:*nn*	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

Command Default

The VPLS ID is generated automatically by VPLS Autodiscovery.

Command Modes

L2 VFI configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

VPLS Autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol BGP autonomous system number and the configured VFI VPN ID. You can use the **vpls-id** command to change the automatically generated VPLS ID.

The Label Distribution Protocol (LDP) uses the VPLS ID when signaling VPLS autodiscovered neighbors. The VPLS ID identifies the VPLS domain.

Only one VPLS ID can be configured per virtual forwarding instance (VFI), and the same VPLS ID cannot be configured in multiple VFIs on the same provider edge (PE) router.

The manually configured VPLS ID replaces the internally generated VPLS ID. The manually configured VPLS ID also changes the automatically generated route target (RT).

The **vpls-id** command defines the attachment group identifier (AGI) for the VPLS domain. Therefore, all provider edge (PE) routers in the same VPLS domain must use the same VPLS ID.

For interautonomous system configurations, you must manually configure the VPLS ID instead of using the automatically generated VPLS ID, because all PE routers do not share the same autonomous system number.

Examples

The following example sets the VPLS ID to the autonomous system and network number 5:300:

```
vpls-id 5:300
```

The following example sets the VPLS ID to IP address and network number 10.4.4.4:70:

```
vpls-id 10.4.4.4:70
```

Related Commands

Command	Description
rd	Creates routing and forwarding tables for a VRF.

waas cm-register url

To register a device with the WAAS Central Manager, use the **waas cm-register url** command in privileged EXEC mode.

waas cm-register url *url port-number*

Syntax Description

url *url*	URL of the device to be registered.
port-number	The port number.

Command Default

No devices are registered with the WAAS Central Manager.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to register a device with the WAAS Central Manager. Before enabling this command, the WCM certificate must be installed on the router.

Note The registration may fail if the port number is not specified.

The values for the *url* argument can be one of the following:

- **archive**
- **cns**
- **flash**
- **ftp**
- **http**
- **https**
- **null**
- **nvram**
- **rcp**
- **scp**
- **system**
- **tar**
- **tftp**
- **tmpsys**

- **xmodem**
- **ymodem**

Examples

The following example shows how to register a device with the WAAS Central Manager:

```
Router> enable
Router# waas cm-register url https://192.0.2.1:8443/wcm/register
```

Related Commands

Command	Description
clear waas	Clears WAAS Express statistics and closed connections information.
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.
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 config

To restore or remove WAAS Express default configurations, use the **waas config** command in privileged EXEC mode.

waas config {**restore-default** | **remove-all**}

Syntax Description

restore-default	Restores the default configuration.
remove-all	Removes all configurations.

Command Default

WAAS Express default configurations are not modified.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to either restore the default configurations or remove the configurations. This command works only if WAAS Express is not enabled on any interface.

Examples

The following example shows how to restore the WAAS Express default configuration:

```
Router> enable
Router# waas config restore-default
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
parameter-map type waas	Configures WAAS Express global parameters.
policy-map type waas	Configures a WAAS Express policy map.
waas enable	Enables WAAS Express on a network interface of a router.
waas export	Associates a NetFlow exporter with WAAS Express.

waas export

To associate a NetFlow exporter with WAAS Express, use the **waas export** command in global configuration mode. To remove the association, use the **no** form of this command.

waas export {**name** *exporter-name* | **timeout** *seconds*}

no waas export {**name** *exporter-name* | **timeout** *seconds*}

Syntax Description

name *exporter-name*	Specifies the name of the exporter.
timeout *seconds*	Specifies the timeout value, in seconds. The default is 300.

Command Default

No NetFlow exporter is associated.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to associate a NetFlow exporter with WAAS Express and export fields to NetFlow v9 records. Use the *seconds* argument to set the timeout value for exporting a long-living connection.

Examples

The following example shows how to associate a NetFlow exporter named exporter1:

```
Router> enable
Router# configure terminal
Router(config)# waas export name exporter1
Router(config)# destination 192.168.1.1
```

Related Commands

Command	Description
class-map type waas	Configures a WAAS Express class map.
flow-sampler	Defines a flow sampler map for random sampled NetFlow accounting to an interface.
flow exporter	Creates a flow exporter.
parameter-map type waas	Configures WAAS Express global parameters.
policy-map type waas	Configures a WAAS Express policy map.
waas config	Restores or removes WAAS Express default configurations.
waas enable	Applies WAN optimization on a network interface of a device.

waas export

To associate a NetFlow exporter with WAAS Express which is used to export WAAS fields in the NetFlow v9 records, use the **waas export** command in global configuration mode. To remove the association, use the **no** form of this command.

waas export {**name** *exporter-name* | **timeout** *timeout-value*}

no waas export {**name** *exporter-name* | **timeout** *timeout-value*}

Syntax Description

name *exporter-name*	Specifies the name of the exporter.
timeout *timeout-value*	Specifies the timeout value. The default is 300 seconds.

Command Default

NetFlow exporter is not associated.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to associate a NetFlow exporter with WAAS Express and export fields to NetFlow v9 records. Use the *timeout* argument to set the timeout value for exporting long living connection.

Examples

The following example shows how to associate a NetFlow exporter named exporter1.

```
Router> enable
Router# configure terminal
Router(config)# flow exporter exporter1
Router(config)# destination 209.165.200.225
Router(config)# waas export name exporter1
```

Related Commands

Command	Description
class-map type waas	Configures WAAS Express class-map.
flow-sampler	Defines a flow sampler map for random sampled NetFlow accounting to an interface.
flow exporter	Creates a flow exporter.
parameter-map type waas	Configures WAAS Express global parameters.
policy-map type waas	Configures an WAAS Express policy-map.
waas config	Restores or removes WAAS Express default configurations.
waas enable	Applies WAN optimization on a network interface of a device.

x25 accept-reverse

To configure the Cisco IOS software to accept all reverse-charge calls, use the **x25 accept-reverse** command in interface or X.25 profile configuration mode. To disable this facility, use the **no** form of this command.

x25 accept-reverse

no x25 accept-reverse

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration
X.25 profile 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

This command causes the interface to accept reverse-charge calls by default. You can also configure this behavior for each peer with the **x25 map** interface configuration command.

Examples

The following example sets acceptance of reverse-charge calls:

```
interface serial 0
 x25 accept-reverse
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.

x25 address

To set the X.121 address of a particular network interface, use the **x25 address** command in interface or X.25 profile configuration mode.

x25 address *x121-address*

Syntax Description

x121-address	Variable-length X.121 address. It is assigned by the X.25 network service provider.

Defaults

Defense Data Network (DDN) and Blacker Front End (BFE) encapsulations have a default interface address generated from the interface IP address. For proper DDN or BFE operation, this generated X.121 address must not be changed. Standard X.25 encapsulations do not have a default.

Command Modes

Interface configuration

X.25 profile 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

When you are connecting to a public data network (PDN), the PDN administrator will assign the X.121 address to be used. Other applications (for example, a private X.25 service), may assign arbitrary X.121 addresses as required by the network and service design. X.25 interfaces that engage in X.25 switching only do not need to assign an X.121 address.

Examples

The following example sets the X.121 address for the interface:

```
interface serial 0
 encapsulation x25
 x25 address 00000123005
```

The address must match that assigned by the X.25 network service provider.

x25 address (line)

To assign an X.121 address to a TTY line, use the **x25 address** command in line configuration mode. To remove the assigned address, use the **no** form of this command.

x25 address *x121-address*

no x25 address *x121-address*

Syntax Description

x121-address	X.121 address. The address must be a numerical string no longer than 20 digits.

Command Default

No X.121 address is defined.

Command Modes

Line configuration

Command History

Release	Modification
12.3(11)YN	This command was introduced.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Usage Guidelines

Each X.121 address can be associated with only one line.

This command cannot configure VTY lines.

Examples

The following example assigns the X.121 address of 12345 to the TTY line:

```
x25 address 12345
```

Related Commands

Command	Description
x25 address	Sets the X.121 address of a particular network interface.

x25 alias

To configure an interface alias address that will allow this interface to accept calls with other destination addresses, use the **x25 alias** command in interface or X.25 profile configuration mode.

x25 alias {*destination-pattern* | *x121-address-pattern*} [**cud** *cud-pattern*]

Syntax Description

destination-pattern	Regular expression used to match against the destination address of a received call.
x121-address-pattern	Alias X.121 address for the interface, allowing it to act as destination host for calls having different destination address.
cud *cud-pattern*	(Optional) Call user data (CUD) pattern, a regular expression of ASCII text. The CUD field might be present in a call packet. The first few bytes (commonly 4 bytes long) identify a protocol; the specified pattern is applied to any user data after the protocol identification.

Defaults

No alias is configured.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
11.2	This command was introduced. It replaces the functionality that was provided by the **alias** keyword of the **x25 route** command.
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

Encapsulation, packet assembler/disassembler (PAD), and Qualified Logical Link Control (QLLC) calls are normally accepted when the destination address is that of the interface (or the zero-length address). Those calls will also be accepted when the destination address matches a configured alias.

Examples

An X.25 call may be addressed to the receiving interface; calls addressed to the receiving interface are eligible for acceptance as a datagram encapsulation, PAD or QLLC connection, and may not be routed. In the following example, serial interface 0 is configured with a native address of 0000123 and a destination alias for any address that starts with 1111123. That is, serial interface 0 can accept its own calls and calls for any destination that starts with 1111123.

```
interface serial 0
 encapsulation x25
 x25 address 0000123
 x25 alias ^1111123.*
```

x25 bfe-decision

Note Effective with Cisco IOS Release 12.2, the **x25 bfe-decision** command is not available in Cisco IOS Software.

To specify how a router configured for **x25 bfe-emergency decision** will participate in emergency mode, use the **x25 bfe-decision** command in interface configuration mode.

x25 bfe-decision {**no** | **yes** | **ask**}

Syntax Description

no	Prevents the router from participating in emergency mode and from sending address translation information to the BFE device.
yes	Allows the router to participate in emergency mode and to send address translation information to the BFE when the BFE enters emergency mode. This information is obtained from the table created by the **x25 remote-red** command.
ask	Configures the Cisco IOS software to prompt you to enter the **bfe** EXEC command.

Command Default

The router does not participate in emergency mode.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example configures serial interface 0 to require an EXEC command from you before it participates in emergency mode. The host IP address is 21.0.0.12, and the address of the remote BFE unit is 21.0.0.1. When the BFE enters emergency mode, the Cisco IOS software prompts you for the **bfe enter** EXEC command to direct the router to participate in emergency mode.

```
interface serial 0
 x25 bfe-emergency decision
 x25 remote-red 21.0.0.12 remote-black 21.0.0.1
 x25 bfe-decision ask
```

Related Commands

Command	Description
bfe	Allows the router to participate in emergency mode or to end participation in emergency mode when the interface is configured using the **x25 bfe-emergency decision** and **x25 bfe-decision ask** commands.
x25 bfe-emergency	Configures the circumstances under which the router participates in emergency mode.
x25 remote-red	Sets up the table that lists the BFE nodes (host or gateways) to which the router will send packets.

x25 bfe-emergency

Note Effective with Cisco IOS Release 12.2, the **x25 bfe-emergency** command is not available in Cisco IOS Software.

To configure the circumstances under which the router participates in emergency mode, use the **x25 bfe-emergency** command in interface configuration mode.

x25 bfe-emergency {**never** | **always** | **decision**}

Syntax Description

never	Prevents the router from sending address translation information to the Blacker Front End (BFE). If it does not receive address translation information, the BFE cannot open a new connection for which it does not know the address.
always	Allows the router to pass address translations to the BFE when it enters emergency mode and an address translation table has been created.
decision	Directs the router to wait until it receives a diagnostic packet from the BFE device indicating that the emergency mode window is open. The window is only open when a condition exists that allows the BFE to enter emergency mode. When the diagnostic packet is received, the participation in emergency mode depends on how the router is configured with the **x25 bfe-decision** command.

Defaults

No address translation information is sent to the BFE.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example configures serial interface 0 to require an EXEC command from you before it participates in emergency mode. The host IP address is 21.0.0.12, and the address of the remote BFE unit is 21.0.0.1. When the BFE enters emergency mode, the Cisco IOS software prompts you for the **bfe enter** EXEC command to direct the router to participate in emergency mode.

```
interface serial 0
 x25 bfe-emergency decision
 x25 remote-red 21.0.0.12 remote-black 21.0.0.1
 x25 bfe-decision ask
```

Related Commands

Command	Description
bfe	Allows the router to participate in emergency mode or to end participation in emergency mode when the interface is configured using the **x25 bfe-emergency decision** and **x25 bfe-decision ask** commands.
x25 bfe-decision	Specifies how a router configured for X.25 BFE emergency decision will participate in emergency mode.

x25 call-record

To enable a record to be made of outgoing, incoming, and switched calls on the router, use the **x25 call-record** command in global configuration mode. To disable such record-making, use the **no** form of this command.

x25 call-record

no x25 call-record

Syntax Description

This command has no arguments or keywords.

Command Default

No call record is generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Cisco recommends that you configure the router to use Syslog Facility to send the generated call records automatically to a remote syslog server for immediate storage and subsequent retrieval. You'll find instructions on how to do that in the *X.25 Call Record* document.

Examples

```
The following example enables generation of records about calls arriving, leaving, or
being switched at the router:

x25 call-record
```

Following are two records generated by one such call, which arrived on an intermediate router's serial interface and departed through XOT, being routed over a hunt group:

Record of the Incoming VC: Example

```
Jun  7 10:42:00.131: %X25-5-CALL_RECORD:
Start=10:41:54.187 UTC Wed Jun 7 2006, End=10:42:00.131 UTC Wed Jun 7 2006,
Host=R3845-86-34, Client=Switch,
Call-direction=incoming,  Calling-addr=33030,  Called-addr=3500,
Interface=Serial0/3/1,  Logical-channel=1024,
Facilities=win-in 2, win-out 2, pkt-in 128, pkt-out 128 tput-in 0, tput-out 0, fast-select
    no, reverse-charging no,
Bytes sent/rcvd=52/55, Packets sent/rcvd=3/3,
Clear cause=0, Diag code=0
```

Record of the Outgoing VC: Example

```
Jun  7 10:42:00.131: %X25-5-CALL_RECORD:
Start=10:41:54.187 UTC Wed Jun 7 2006, End=10:42:00.131 UTC Wed Jun 7 2006,
Host=R3845-86-34, Client=Switch, Huntgroup=HG4,
Call-direction=outgoing,  Calling-addr=33030,  Called-addr=3500,
Interface=XOT (local: 10.2.86.34:23686 remote: 10.2.86.35:1998),  Logical-channel=1,
Facilities=win-in 2, win-out 2, pkt-in 128, pkt-out 128 tput-in 0, tput-out 0, fast-select
    no, reverse-charging no,
Bytes sent/rcvd=55/52, Packets sent/rcvd=3/3,
Clear cause=0, Diag code=0
```

Related Commands

Command	Description
logging host	Enables logging to a remote syslog server.

x25 default

To set a default protocol that Cisco IOS software will assume applies to incoming calls with unknown or missing protocol identifier in the call user data (CUD), use the **x25 default** command in interface configuration mode or X.25 profile configuration mode. To remove the default protocol specified, use the **no** form of this command.

x25 default *protocol*

no x25 default *protocol*

Syntax Description

protocol	Specifies the protocol to assume; may be **ip** or **pad**.

Defaults

No default protocol is specified.

Command Modes

Interface configuration

X.25 profile 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

This command specifies the protocol assumed by the Cisco IOS software for incoming calls with unknown or missing protocol identifier in the call user data (CUD). If you do not use the **x25 default** interface configuration command, the software clears any incoming calls with unrecognized CUD.

Examples

The following example establishes IP as the default protocol for X.25 calls:

```
interface serial 0
 x25 default ip
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.

x25 facility

To force facilities on a per-call basis for calls originated by the router (switched calls are not affected), use the **x25 facility** command in interface or X.25 profile configuration mode. To disable a facility, use the **no** form of this command.

x25 facility *option*

no x25 facility *option*

Syntax Description

option	Set of user facilities options. See Table 107 for a list of supported facilities and their values.

Defaults

No facility is sent.

Command Modes

Interface configuration
X.25 profile 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

Table 107 lists the set of **x25 facility** command user facilities options.

Table 107 x25 facility User Facilities Options

User Facilities Option	Description
cug *number*	Specifies a closed user group (CUG) number; CUGs numbered from 1 to 9999 are allowed. CUGs can be used by a public data network (PDN) to create a virtual private network within the larger network and to restrict access.
packetsize *in-size out-size*	Proposes input maximum packet size *(in-size*) and output maximum packet size (*out-size*) for flow control parameter negotiation. Both values must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
windowsize *in-size out-size*	Proposes the packet count for input windows (*in-size*) and output windows (*out-size*) for flow control parameter negotiation. Both values must be in the range 1 to 127 and must not be greater than or equal to the value set for the **x25 modulo** command.
reverse	Specifies reverses charging on all calls originated by the interface.

Table 107 x25 facility User Facilities Options (continued)

User Facilities Option	Description
throughput *in out*	Sets the requested throughput class negotiation values for input (*in*) and output (*out*) throughput across the network. Values for *in* and *out* are in bits per second (bps) and range from 75 to 64000 bps.
transit-delay *value*	Specifies a network transit delay to request for the duration of outgoing calls for networks that support transit delay. The transit delay value can be between 0 and 65534 milliseconds.
roa *name*	Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operation Agencies (ROAs) to use in outgoing Call Request packets.

Examples

The following example specifies a transit delay value in an X.25 configuration:

```
interface serial 0
 x25 facility transit-delay 24000
```

The following example sets an ROA name and then sends the list via the X.25 user facilities:

```
x25 roa green_list 23 35 36
interface serial 0
 x25 facility roa green_list
```

Related Commands

Command	Description
x25 suppress-called-address	Omits the destination address in outgoing calls.

x25 fail-over

To configure a secondary interface and set the number of seconds for which a primary interface must be up before the secondary interface resets, use the **x25 fail-over** command in the appropriate configuration mode. To prevent the secondary interface from resetting, use the **no** form of this command.

x25 fail-over *seconds* **interface** *type number* [*dlci* | *mac-address*]

no x25 fail-over *seconds* **interface** *type number* [*dlci* | *mac-address*]

Syntax Description

seconds	Number of seconds for which the primary interface must be up before the secondary interface resets.
interface	Secondary interface.
type	Interface type.
number	Interface number.
dlci	(Optional) DLCI number.
mac-address	(Optional) MAC address.

Defaults

No default behavior or values

Command Modes

Interface configuration
X.25 profile configuration

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

The **x25 fail-over** command can be configured on a primary X.25 interface or an X.25 profile only.

Examples

In the following example, X.25 failover is configured on a network that is also configured for Annex G. If data-link connection identifier (DLCI) 13 or DLCI 14 on serial interface 1/0 goes down, dialer interface 1 will serve as the secondary interface. After DLCI 13 or 14 comes back up and remains up for 20 seconds, dialer interface 1 will reset, sending all calls back to the primary interface.

```
interface serial1/0
 encapsulation frame-relay
 frame-relay interface-dlci 13
 x25-profile frame1
  exit
 frame-relay interface-dlci 14
```

```
 x25-profile frame1 dte
  exit
!
interface dialer1
 encapsulation x25
 exit

x25 route ^1234 interface serial1/0 dlci 13
x25 route ^1234 interface serial1/0 dlci 14
x25 route ^1234 interface dialer1
!
x25 profile frame1
 x25 fail-over 20 interface dialer1
  exit
!
```

Related Commands

Command	Description
show x25 context	Displays information about X.25 links.
x25 profile	Configures an X.25 profile without specifying any hardware-specific information.

x25 hic

To set the highest incoming-only virtual circuit (VC) number, use the **x25 hic** interface configuration command.

x25 hic *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.

Defaults

0

Command Modes

Interface configuration
X.25 profile 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

This command is applicable only if you have the X.25 switch configured for an incoming-only VC range. *Incoming* is from the perspective of the X.25 data terminal equipment (DTE). If you do not want any outgoing calls from your DTE, configure both ends to disable the two-way range (set the values of **x25 ltc** and **x25 htc** to 0) and configure an incoming-only range. Any incoming-only range must come before (that is, must be numerically less than) any two-way range. Any two-way range must come before any outgoing-only range.

Examples

The following example sets a valid incoming-only VC range of 1 to 5:

```
interface serial 0
 x25 lic 1
 x25 hic 5
```

Related Commands

Command	Description
x25 lic	Sets the lowest incoming-only VC number.

x25 hoc

To set the highest outgoing-only virtual circuit (VC) number, use the **x25 hoc** interface configuration command.

x25 hoc *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.

Defaults

0

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

This command is applicable only if you have the X.25 switch configured for an outgoing-only VC range. *Outgoing* is from the perspective of the X.25 data terminal equipment (DTE). If you do not want any incoming calls on your DTE, disable the two-way range (set the values of **x25 ltc** and **x25 htc** to 0) and configure an outgoing-only range. Any outgoing-only range must come after (that is, be numerically greater than) any other range.

Examples

The following example sets a valid outgoing-only VC range of 2000 to 2005:

```
interface serial 0
 x25 loc 2000
 x25 hoc 2005
```

Related Commands

Command	Description
x25 loc	Sets the lowest outgoing-only VC number.

x25 hold-queue

To set the maximum number of packets to hold until a virtual circuit (VC) is able to send, use the **x25 hold-queue** command in interface configuration mode. To remove this command from the configuration file and restore the default value, use the **no** form of this command without an argument.

x25 hold-queue *packets*

no x25 hold-queue [*packets*]

Syntax Description

packets	Number of packets. A hold queue value of 0 allows an unlimited number of packets in the hold queue.

Defaults

10 packets

Command Modes

Interface configuration
X.25 profile 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

If you set the *queue-size* argument to 0 when using the **no x25 hold-queue** command, there will be no hold queue limit. While this setting will prevent drops until the router runs out of memory, it is only rarely appropriate. A VC hold queue value is determined when it is created; changing this parameter will not affect the hold queue limits of the existing virtual circuits.

Examples

The following example sets the X.25 hold queue to hold 25 packets:

```
interface serial 0
 x25 hold-queue 25
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.
x25 ips	Sets the interface default maximum input packet size to match that of the network.
x25 ops	Sets the interface default maximum output packet size to match that of the network.

x25 hold-vc-timer

To start the timer that prevents additional calls to a destination for a given period of time (thus preventing overruns on some X.25 switches caused by Call Request packets), use the **x25 hold-vc-timer** command in interface configuration mode. To restore the default value for the timer, use the **no** form of this command.

x25 hold-vc-timer *minutes*

no x25 hold-vc-timer

Syntax Description

minutes	Number of minutes that calls to a previously failed destination will be prevented. Incoming calls are still accepted.

Defaults

0 minutes

Command Modes

Interface configuration
X.25 profile 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

Only Call Requests that the router originates are held down; routed X.25 Call Requests are not affected by this parameter.

Upon receiving a Clear Request for an outstanding Call Request, the X.25 support code immediately tries another Call Request if it has more traffic to send, and this action might cause overrun problems.

Examples

The following example sets this timer to 3 minutes:

```
interface serial 0
 x25 hold-vc-timer 3
```

x25 host

To define a static host name-to-address mapping, use the **x25 host** command in global configuration mode. To remove the host name, use the **no** form of the command.

x25 host *name x121-address* [**cud** *call-user-data*]

no x25 host *name*

Syntax Description

name	Host name.
x121-address	The X.121 address.
cud *call-user-data*	(Optional) Sets the Call User Data (CUD) field in the X.25 Call Request packet.

Defaults

No static host name-to-address mapping is defined.

Command Modes

Global 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

This command permits you to map an X.121 address to an easily recognizable name. You can later use this host name instead of the X.121 address when you issue the **translate** command for X.25.

Examples

The following example specifies a static address mapping:

```
x25 host Willard 4085551212
```

The following example removes a static address mapping:

```
no x25 host Willard
```

The following example specifies static address mapping from the X.121 address 12345678 to the host name “ocean”. It then uses the name “ocean” in the **translate** command in place of the X.121 address when translating from the X.25 host to the PPP host with address 10.0.0.2.

```
x25 host ocean 12345678
translate x25 ocean ppp 10.0.0.2 routing
```

Related Commands

Command	Description
translate x25	Translates a request to another outgoing protocol connection type when that X.25 connection request to a particular destination address is received.

x25 htc

To set the highest two-way virtual circuit (VC) number, use the **x25 htc** command in interface configuration mode or X.25 profile configuration mode.

x25 htc *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no two-way VC range.

Defaults

1024 for X.25 network service interfaces; 4095 for CMNS network service interfaces.

Command Modes

Interface configuration
X.25 profile 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

This command is applicable if the X.25 switch is configured for a two-way VC range. Any two-way VC range must come after (that is, be numerically larger than) any incoming-only range, and must come before any outgoing-only range.

Examples

The following example sets a valid two-way VC range of 5 to 25:

```
interface serial 0
 x25 ltc 5
 x25 htc 25
```

Related Commands

Command	Description
cmns enable	Enables the CMNS on a nonserial interface.
x25 ltc	Sets the lowest two-way VC number.

x25 hunt-group

To create and maintain a hunt group, use the **x25 hunt-group** command in global configuration mode. To delete this hunt group, use the **no** form of this command.

x25 hunt-group *name* {**rotary | vc-count**}

no x25 hunt-group *name*

Syntax Description

name	Name you assign to the particular hunt group.
rotary	Each call steps to the next interface.
vc-count	Each call is placed on the interface with most available logical channels.

Defaults

No X.25 hunt group is created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)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

Only one load-balancing distribution method can be selected for a hunt group, although one interface can participate in one or more hunt groups.

The rotary distribution method sends every call to the next available interface regardless of line speed and the number of available VCs on that interface.

The vc-count distribution method sends calls to the interface with the largest number of available logical channels. This method ensures a good load balance when you have lines of equal speed. If the line speeds are unequal, the vc-count method will favor the line with the higher speed. In cases where interfaces have the same line speed, the call is sent to the interface that is defined earliest in the hunt group.

To distribute calls equally among interfaces regardless of line speed, configure each interface with the same number of VCs.

With the vc-count distribution method, if a hunt group does not contain an operational interface, the call will be forwarded to the next route if one was specified. If a session is terminated on an interface within the hunt group, that interface now has more available VCs and it will be chosen next.

Examples

X.25 Load Balancing Using VC-Count Distribution Method: Example

In the following example, the vc-count distribution method is used on a hunt group that contains two serial interfaces that have different numbers of VCs. Assuming no sessions are being terminated at this time, the first 450 calls will be sent to Serial1, and subsequent calls will alternate between Serial0 and Serial1 until the interfaces are full.

```
interface serial0
  description 56k link supporting 50 virtual circuits
  x25 htc 50
!
interface serial1
  description T1 line supporting 500 virtual circuits
  x25 htc 500
!
x25 hunt-group hg-vc vc-count
  interface serial0
  interface serial1
!
```

Hunt Group Configuration: Example

The following example shows the creation of hunt group “HG1” with serial interfaces 1 and 2 and two specific XOT target IP addresses (172.17.125.54 and 172.17.125.34). Hunt group "HG1" is configured to use rotary distribution method. The example also shows the creation of hunt group “HG2” with serial interfaces 0 and 3. Hunt group "HG2" will use vc-count distribution method.

```
x25 hunt-group HG1 rotary
 interface serial 1
 interface serial 2
 xot 172.17.125.54
 xot 172.17.125.34
 exit
x25 hunt-group HG2 vc-count
 interface serial 0
 interface serial 3
```

Related Commands

Command	Description
show x25 hunt-group	Displays X.25 hunt groups, detailed interface statistics, and distribution methods.

x25 idle

To define the period of inactivity after which the router can clear a switched virtual circuit (SVC), use the **x25 idle** command in interface configuration mode.

x25 idle *minutes* [*seconds*]

Syntax Description

minutes	Idle period in minutes. Accepted range for the *minutes* argument is from 0 to 255 minutes. The default is 0 minutes, which keeps an SVC open indefinitely.
seconds	(Optional) Idle period in seconds. Adds granularity to the idle period of X.25 encapsulation virtual circuits (VCs) only. Accepted range is from 1 to 59 seconds. **Note** Set the *minutes* argument to 0, if the desired idle period on the X.25 encapsulation VC is fewer than 60 seconds, then enter a value for the optional *seconds* argument. The *seconds* argument will be ignored for other types of X.25 VCs such as packet assembler/disassembler (PAD) and protocol translation VCs.

Defaults

0 minutes (the SVC is kept open indefinitely)

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
10.0	This command was introduced.
12.4(6)T	This command was enhanced with the *seconds* argument, for finer granularity in setting the idle period for X.25 encapsulation VCs.
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

Calls originated and terminated by the router are cleared; packet assembler/disassembler and switched virtual circuits are not affected. To clear one or all virtual circuits at once, use the **clear x25** privileged EXEC command. Use the **show interfaces** and **show x25 vc** privileged EXEC commands to display the configured timeout values.

Examples

The following example sets a 5-minute wait period before an idle circuit is cleared:

```
interface serial 2
 x25 idle 5
```

The following example clears an X.25 encapsulation VC after the VC remains idle for 1 minute and 10 seconds:

```
interface Serial0/0
 description connects to tester s1/0
 ip address 10.132.0.8 255.255.255.0
 encapsulation x25
 x25 address 2xx8xx
 x25 idle 1 10
 x25 map ip 10.132.0.9 2xx9xx
 clock rate 64000
end
```

The **x25 idle 0 30** command would change this configuration to clear the X.25 encapsulation VC after the VC remains idle for 30 seconds. See the description for the **x25 map** command for information on setting the idle timer using that command.

Related Commands

Command	Description
clear x25	Restarts an X.25 or CMNS service, clears an SVC, or resets a PVC.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show x25 vc	Displays information about active SVCs and PVCs.
x25 map	Sets up the LAN protocols-to-remote-host mapping.

x25 ip-precedence

To enable the Cisco IOS software to use the IP precedence value when it opens a new virtual circuit (VC), use the **x25 ip-precedence** command in interface configuration mode. To cause the Cisco IOS software to ignore the precedence value when opening VCs, use the **no** form of this command.

x25 ip-precedence

no x25 ip-precedence

Syntax Description

This command has no arguments or keywords.

Defaults

The router opens one VC for all types of service.

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

This feature is useful only for Defense Data Network (DDN) or Blacker Front End (BFE) encapsulations because only these methods have an IP precedence facility defined to allow the source and destination devices to both use the VC for traffic of the given IP priority.

Verify that your host does not send nonstandard data in the IP type of service (TOS) field because it can cause multiple wasteful virtual circuits to be created.

Four VCs may be opened based on IP precedence to encapsulate routine, priority, immediate, and all higher precedences.

The **x25 map nvc** limit or the default **x25 nvc** limit still applies.

Examples

The following example allows new IP encapsulation VCs based on the IP precedence:

```
interface serial 3
 x25 ip-precedence
```

x25 ips

To set the interface default maximum input packet size to match that of the network, use the **x25 ips** interface configuration command.

x25 ips *bytes*

Syntax Description

bytes	Byte count. It can be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.

Defaults

128 bytes

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

X.25 network connections have a default maximum input packet size set by the network administrator. Larger packet sizes require less overhead processing. To send a packet larger than the X.25 packet size over an X.25 virtual circuit, the Cisco IOS software must break the packet into two or more X.25 packets with the more data bit (M-bit) set. The receiving device collects all packets with the M-bit set and reassembles the original packet.

Note Set the **x25 ips** and **x25 ops** commands to the same value unless your network supports asymmetric input and output packet sizes.

Examples

The following example sets the default maximum packet sizes to 512:

```
interface serial 1
 x25 ips 512
 x25 ops 512
```

Related Commands

Command	Description
x25 facility	Forces facilities on a per-call basis for calls originated by the router (switched calls are not affected).
x25 ops	Sets the interface default maximum output packet size to match that of the network.

x25 lic

To set the lowest incoming-only virtual circuit (VC) number, use the **x25 lic** interface configuration command.

x25 lic *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no incoming-only VC range.

Defaults

0

Command Modes

Interface configuration
X.25 profile 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

This command is applicable only if you have the X.25 switch configured for an incoming-only VC range. *Incoming* is from the perspective of the X.25 DTE device. If you do not want any outgoing calls on your DTE device, disable the two-way range (set the values of **x25 ltc** and **x25 htc** to 0).

The following example sets a valid incoming-only VC range of 1 to 5, and sets the lowest two-way VC number:

```
interface serial 0
 x25 lic 1
 x25 hic 5
 x25 ltc 6
```

Related Commands

Command	Description
x25 hic	Sets the highest incoming-only VC number.

x25 linkrestart

To force X.25 Level 3 (packet level) to restart when Level 2 (Link Access Procedure, Balanced [LAPB], the link level) resets, use the **x25 linkrestart** command in interface configuration mode. To disable this function, use the **no** form of this command.

x25 linkrestart

no x25 linkrestart

Syntax Description

This command has no arguments or keywords.

Defaults

Forcing packet-level restarts is the default and is necessary for networks that expect this behavior.

Command Modes

Interface configuration
X.25 profile 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.

Examples

The following example disables the link-level restart:

```
interface serial 3
 no x25 linkrestart
```

x25 loc

To set the lowest outgoing-only virtual circuit (VC) number, use the **x25 loc** interface configuration command.

x25 loc *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no outgoing-only VC range.

Defaults

0

Command Modes

Interface configuration
X.25 profile 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

This command is applicable only if you have the X.25 switch configured for an outgoing-only VC range. *Outgoing* is from the perspective of the X.25 DTE device. If you do not want any incoming calls from your DTE device, configure the values of **x25 loc** and **x25 hoc** and set the values of **x25 ltc** and **x25 htc** to 0.

Examples

The following example sets a valid outgoing-only virtual circuit range of 2000 to 2005:

```
interface serial 0
 x25 loc 2000
 x25 hoc 2005
```

Related Commands

Command	Description
x25 hoc	Sets the highest outgoing-only VC number.

x25 ltc

To set the lowest two-way virtual circuit (VC) number, use the **x25 ltc** interface configuration command.

x25 ltc *circuit-number*

Syntax Description

circuit-number	VC number from 1 to 4095, or 0 if there is no two-way VC range.

Defaults

1

Command Modes

Interface configuration
X.25 profile 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

This command is applicable if you have the X.25 switch configured for a two-way virtual circuit range. Any two-way virtual circuit range must come after (that is, be numerically larger than) any incoming-only range, and must come before any outgoing-only range.

Examples

The following example sets a valid two-way virtual circuit range of 5 to 25:

```
interface serial 0
 x25 ltc 5
 x25 htc 25
```

Related Commands

Command	Description
x25 htc	Sets the highest two-way VC number.

x25 map

To set up the LAN protocols-to-remote-host mapping, use the **x25 map** command in interface configuration or X.25 profile configuration mode. To retract a prior mapping, use the **no** form of this command.

x25 map *protocol address* [*protocol2 address2* [...[*protocol9 address9*]]] *x121-address* [*option*]

no x25 map *protocol address x121-address*

Syntax Description

protocol	Protocol type, entered by keyword. Supported protocols are entered by keyword, as listed in the Protocols Supported by X.25 table. As many as nine protocol and address pairs (represented by ellipses in the syntax example) can be specified on one command line.
address	Protocol address.
x121-address	X.121 address of the remote host.
option	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in the x25 map Options table.

Defaults

No LAN protocol-to-remote-host mapping is set up.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **apollo**, **vines**, and **xns** arguments were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems are no longer available in the Cisco IOS software.
12.4(6)T	The **idle** option of this command was enhanced to support seconds granularity in setting the idle period.
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

Because no defined protocol can dynamically determine LAN protocol-to-remote-host mappings, you must enter all the information for each host with which the router may exchange X.25 encapsulation traffic.

Two methods are available to encapsulate traffic: Cisco's long-available encapsulation method and the Internet Engineering Task Force (IETF) standard method defined in RFC 1356; the latter allows hosts to exchange several protocols over a single virtual circuit. Cisco's encapsulation method is the default (for backward compatibility) unless the interface configuration command specifies the **ietf** keyword.

When you configure multiprotocol maps, you can specify a maximum of nine protocol and address pairs in an **x25 map** command. A multiprotocol map can specify a single address for all the supported protocols. However, if IP and TCP header compression are both specified, the same IP address must be given for both protocols.

Encapsulation maps might also specify that traffic between the two hosts should be compressed, thus increasing the effective bandwidth between them at the expense of memory and computation time. Because each compression VC requires memory and computation resources, compression must be used with care and monitored to maintain acceptable resource usage and overall performance.

Bridging is supported only if you are using Cisco's traditional encapsulation method. For correct operation, bridging maps must specify the **broadcast** option. Because most datagram routing protocols rely on broadcasts or multicasts to send routing information to their neighbors, the **broadcast** keyword is needed to run such routing protocols over X.25.

Open Shortest Path First (OSPF) Protocol treats a nonbroadcast, multiaccess network such as X.25 in much the same way as it treats a broadcast network by requiring the selection of a designated router. In earlier releases of the Cisco IOS software, this selection required manual assignment in the OSPF configuration using the **neighbor** router configuration command. When the **x25 map** command is included in the configuration with the broadcast, and the **ip ospf network** command with the **broadcast** keyword is configured, there is no need to configure any neighbors manually. OSPF will run over the X.25 network as a broadcast network. (Refer to the **ip ospf network** interface configuration command for more detail.)

Note The OSPF broadcast mechanism assumes that IP class D addresses are never used for regular traffic over X.25.

You can modify the options of an **x25 map** command by restating the complete set of protocols and addresses specified for the map, followed by the desired options. To delete a map command, you must specify the complete set of protocols and addresses; the options can be omitted when deleting a map.

Once defined, a map's protocols and addresses cannot be changed. This requirement exists because the Cisco IOS software cannot determine whether you want to add to, delete from, or modify an existing map's protocol and address specification, or simply have mistyped the command. To change a map's protocol and address specification, you must delete it and create a new map.

A given protocol-address pair cannot be used in more than one map on the same interface.

Table 108 lists the protocols supported by X.25.

Table 108 Protocols Supported by X.25

Keyword	Protocol
appletalk	AppleTalk
bridge	Bridging[1]
clns	ISO Connectionless Network Service
compressedtcp	TCP/IP header compression
decnet	DECnet
ip	IP

Table 108 Protocols Supported by X.25 (continued)

Keyword	Protocol
ipx	Novell IPX
pad	Packet assembler/disassembler (PAD) links[2]
qllc	System Network Architecture (SNA) encapsulation in X.25[3]

1. Bridging traffic is supported only for Cisco's traditional encapsulation method, so a bridge map cannot specify other protocols.
2. PAD maps are used to configure session and protocol translation access, therefore, this protocol is not available for multiprotocol encapsulation.
3. Qualified Logical Link Control (QLLC) is not available for multiprotocol encapsulation.

Note The Connection-Mode Network Service (CMNS) map form is obsolete; its function is replaced by the enhanced **x25 route** command.

Table 109 lists the map options supported by X.25 when you use the **x25 map** command.

Table 109 x25 map Options

Option	Description
accept-reverse	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
broadcast	Causes the Cisco IOS software to direct any broadcasts sent through this interface to the specified X.121 address. This option also simplifies the configuration of OSPF; see "Usage Guidelines" for more detail.
cug *group-number*	Specifies a closed user group (CUG) number (from 1 to 9999) for the mapping in an outgoing call.
compress	Specifies that X.25 payload compression be used for mapping the traffic to this host. Each virtual circuit established for compressed traffic uses a significant amount of memory (for a table of learned data patterns) and for computation (for compression and decompression of all data). Cisco recommends that compression be used with careful consideration of its impact on overall performance.
idle *minutes* [*seconds*]	Idle period in minutes and, optionally, seconds. Accepted range for the *minutes* argument is from 0 to 255 minutes. The default is 0 minutes, which keeps an SVC open indefinitely. Accepted range for the optional *seconds* argument is from 1 to 59 seconds, and the *seconds* argument is valid only for setting the idle period for X.25 encapsulation VCs. **Note** Set the *minutes* argument to 0, if the desired idle period on the X.25 encapsulation VC is fewer than 60 seconds, then enter a value for the optional *seconds* argument.

Table 109 x25 map Options (continued)

Option	Description
method {**cisco** | **ietf** | **snap** | **multi**}	Specifies the encapsulation method. The choices are as follows: • **cisco**—Cisco's proprietary encapsulation; not available if more than one protocol is to be carried. • **ietf**—Default RFC 1356 operation: protocol identification of single-protocol virtual circuits and protocol identification within multiprotocol virtual circuits use the standard encoding, which is compatible with RFC 877. Multiprotocol virtual circuits are used only if needed. • **snap**—RFC 1356 operation where IP is identified with SNAP rather than the standard IETF method (the standard method is compatible with RFC 877). • **multi**—Forces a map that specifies a single protocol to set up a multiprotocol VC when a call is originated; also forces a single-protocol PVC to use multiprotocol data identification methods for all datagrams sent and received.
no-incoming	Uses the map only to originate calls.
no-outgoing	Does not originate calls when using the map.
nudata *string*	Specifies the network user identification in a format determined by the network administrator (as allowed by the standards). This option is provided for connecting to non-Cisco equipment that requires an NUID facility. The string should not exceed 130 characters and must be enclosed in quotation marks (" ") if there are any spaces present. This option only works only if the router is configured as an X.25 DTE.
nuid *username password*	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified TACACS username and password (in a format defined by Cisco). This option should be used only when connecting to another Cisco router. The combined length of the username and password should not exceed 127 characters. This option works only if the router is configured as an X.25 DTE.
nvc *count*	Sets the maximum number of virtual circuits for this map or host. The default *count* is the **x25 nvc** setting of the interface. A maximum number of eight virtual circuits can be configured for each map. Compressed TCP may use only one virtual circuit.
packetsize *in-size out-size*	Proposes maximum input packet size (*in-size*) and maximum output packet size (*out-size*) for an outgoing call. Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
passive	Specifies that the X.25 interface should send compressed outgoing TCP datagrams only if they were already compressed when they were received. This option is available only for compressed TCP maps.
reverse	Specifies reverse charging for outgoing calls.

Table 109 x25 map Options (continued)

Option	Description
roa *name*	Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operating Agencies (ROAs, formerly called Recognized Private Operating Agencies, or RPOAs) to use in outgoing Call Request packets.
throughput *in out*	Sets the requested throughput class values for input (*in*) and output (*out*) throughput across the network for an outgoing call. Values for *in* and *out* are in bits per second (bps) and range from 75 to 48000 bps.
transit-delay *milliseconds*	Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
windowsize *in-size out-size*	Proposes the packet count for input window (*in-size*) and output window (*out-size*) for an outgoing call. Both values typically are the same, must be in the range 1 to 127, and must be less than the value set by the **x25 modulo** command.

Examples

The following example maps IP address 172.20.2.5 to X.121 address 000000010300. The **broadcast** keyword directs any broadcasts sent through this interface to the specified X.121 address.

```
interface serial 0
 x25 map ip 172.20.2.5 000000010300 broadcast
```

The following example specifies an ROA name to be used for originating connections:

```
x25 roa green_list 23 35 36
interface serial 0
 x25 map ip 172.20.170.26 10 roa green_list
```

The following example specifies an NUID facility to send on calls originated for the address map:

```
interface serial 0
 x25 map ip 172.20.174.32 2 nudata “Network User ID 35”
```

Strings can be quoted, but quotation marks are not required unless embedded blanks are present.

In the following example, the VC times out 10 seconds after the circuit becomes idle (the setting configured in the **x25 map** command, rather than the **x25 idle** command):

```
interface Serial0/0
 description connects to tester s1/0
 ip address 10.132.0.8 255.255.255.0
 encapsulation x25 dce
 x25 address 2xx8xx
 x25 idle 0 20
 x25 map ip 10.132.0.9 2xx9xx idle 0 10
 clock rate 64000
end
```

The settings for the **x25 map** command have higher precedence over the timeout period configured using the **x25 idle** command.

Related Commands

Command	Description
ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.
show x25 map	Displays information about configured address maps.
x25 facility	Forces facilities on a per-call basis for calls originated by the router.
x25 idle	Defines the period of inactivity after which the router can clear an SVC.
x25 map bridge	Configures an Internet-to-X.121 address mapping for bridging over X.25.
x25 map compressedtcp	Maps compressed TCP traffic to an X.121 address.
x25 map pad	Configures an X.121 address mapping for PAD access over X.25.
x25 route	Creates an entry in the X.25 routing table.
x25 suppress-called-address	Omits the destination address in outgoing calls.

x25 map bridge

To configure an Internet-to-X.121 address mapping for bridging of packets in X.25 frames, use the **x25 map bridge** command in interface configuration mode. To disable the Internet-to-X.121 address mapping, use the **no** form of this command.

x25 map bridge *x121-address* **broadcast** [*option*]

Syntax Description

x121-address	The X.121 address.
broadcast	Required keyword for bridging over X.25.
option	(Optional) Services that can be added to this map (same options as the **x25 map** command). See Table 6 for more details.

Defaults

No bridging over X.25 is configured.

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

The X.25 bridging software uses the same spanning-tree algorithm as the other bridging functions, but allows packets to be encapsulated in X.25 frames and transmitted across X.25 media. This command specifies IP-to-X.121 address mapping and maintains a table of both the Ethernet and X.121 addresses.

Table 110 lists **x25 map bridge** options.

Table 110 x25 map bridge Options

Option	Description
accept-reverse	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
broadcast	Causes the Cisco IOS software to direct any broadcasts sent through this interface to the specified X.121 address. This option also simplifies the configuration of Open Shortest Path First (OSPF) Protocol; see “Usage Guidelines” for more detail.

Table 110 x25 map bridge Options (continued)

Option	Description
compress	Specifies that X.25 payload compression be used for mapping the traffic to this host. Each virtual circuit established for compressed traffic uses a significant amount of memory (for a table of learned data patterns) and for computation (for compression and decompression of all data). Cisco recommends that compression be used with careful consideration of its impact on overall performance.
cug *group-number*	Specifies a closed user group (CUG) number (from 1 to 9999) for the mapping in an outgoing call.
idle *minutes*	Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout.
method {**cisco** | **ietf** | **snap** | **multi**}	Specifies the encapsulation method. The choices are as follows: • **cisco**—Cisco's proprietary encapsulation; not available if more than one protocol is to be carried. • **ietf**—Default RFC 1356 operation: protocol identification of single-protocol virtual circuits and protocol identification within multiprotocol virtual circuits use the standard encoding, which is compatible with RFC 877. Multiprotocol virtual circuits are used only if needed. • **snap**—RFC 1356 operation where IP is identified with SNAP rather than the standard Internet Engineering Task Force (IETF) method (the standard method is compatible with RFC 877). • **multi**—Forces a map that specifies a single protocol to set up a multiprotocol virtual circuit when a call is originated; also forces a single-protocol permanent virtual circuit (PVC) to use multiprotocol data identification methods for all datagrams sent and received.
no-incoming	Uses the map only to originate calls.
no-outgoing	Does not originate calls when using the map.
nudata *string*	Specifies the network user identification in a format determined by the network administrator (as allowed by the standards). This option is provided for connecting to non-Cisco equipment that requires an NUID facility. The string should not exceed 130 characters and must be enclosed in quotation marks (" ") if there are any spaces present. This option only works if the router is configured as an X.25 DTE device.
nuid *username password*	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified Terminal Access Controller Access Control System (TACACS) username and password (in a format defined by Cisco). This option should be used only when connecting to another Cisco router. The combined length of the username and password should not exceed 127 characters. This option only works if the router is configured as an X.25 DTE.

Table 110 x25 map bridge Options (continued)

Option	Description
nvc *count*	Sets the maximum number of virtual circuits for this map or host. The default *count* is the **x25 nvc** setting of the interface. A maximum number of eight virtual circuits can be configured for each map. Compressed TCP may use only 1 virtual circuit.
packetsize *in-size out-size*	Proposes maximum input packet size (*in-size*) and maximum output packet size (*out-size*) for an outgoing call. Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
passive	Specifies that the X.25 interface should send compressed outgoing TCP datagrams only if they were already compressed when they were received. This option is available only for compressed TCP maps.
reverse	Specifies reverse charging for outgoing calls.
roa *name*	Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operating Agencies (ROAs, formerly called Recognized Private Operating Agencies, or RPOAs) to use in outgoing Call Request packets.
throughput *in out*	Sets the requested throughput class values for input (*in*) and output (*out*) throughput across the network for an outgoing call. Values for *in* and *out* are in bits per second (bps) and range from 75 to 48000 bps.
transit-delay *milliseconds*	Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
windowsize *in-size out-size*	Proposes the packet count for input window (*in-size*) and output window (*out-size*) for an outgoing call. Both values typically are the same, must be in the range 1 to 127, and must be less than the value set by the **x25 modulo** command.

Examples

The following example configures transparent bridging over X.25 between two Cisco routers using a maximum of six virtual circuits:

```
interface serial 1
 x25 map bridge 000000010300 broadcast nvc 6
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.
x25 address	Sets the X.121 address of a particular network interface.

x25 map cmns

The **x25 map cmns** command is replaced by the enhanced **x25 route** command. See the description of the **x25 route** command in this chapter for more information.

x25 map compressedtcp

To map compressed TCP traffic to an X.121 address, use the **x25 map compressedtcp** command in interface configuration mode. To delete a TCP/IP header compression map for the link, use the **no** form of this command.

x25 map compressedtcp *ip-address* [*protocol2 address2* [...[*protocol9 address9*]]] *x121-address* [*option*]

no x25 map compressedtcp *address* [*protocol2 address2* [...[*protocol9 address9*]]] *x121-address*

Syntax Description

ip-address	IP address.
protocol	(Optional) Protocol type, entered by keyword. Supported protocols are entered by keyword, as listed in Table 108 earlier in this chapter. As many as nine protocol and address pairs can be specified in one command line.
address	(Optional) Protocol address.
x121-address	X.121 address.
option	(Optional) The same options as those for the **x25 map** command; see Table 109 earlier in this chapter.

Defaults

No mapping is configured.

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

Cisco supports RFC 1144 TCP/IP header compression (THC) on serial lines using HDLC and X.25 encapsulation. THC encapsulation is only slightly different from other encapsulation traffic, but these differences are worth noting. The implementation of compressed TCP over X.25 uses one virtual circuit to pass the compressed packets. Any IP traffic (including standard TCP) is separate from TCH traffic; it is carried over separate IP encapsulation virtual circuits or identified separately in a multiprotocol virtual circuit.

Note If you specify both **ip** and **compressedtcp** in the same **x25 map compressedtcp** command, they must both specify the same IP address.

The **nvc** map option cannot be used for TCP/IP header compression, because only one virtual circuit can carry compressed TCP/IP header traffic to a given host.

Examples

The following example establishes a map for TCP/IP header compression on serial interface 4:

```
interface serial 4
 ip tcp header-compression
 x25 map compressedtcp 172.20.2.5 000000010300
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.

x25 map pad

To configure an X.121 address mapping for packet assembler/disassembler (PAD) access over X.25, use the **x25 map pad** interface configuration command.

x25 map pad *x121-address* [*option*]

Syntax Description

x121-address	X.121 address of the interface.
option	(Optional) Services that can be added to this map—the same options as the **x25 map** command; see Table 109 earlier in this chapter.

Defaults

No specific options are used for PAD access.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	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

Use a PAD map to configure optional X.25 facility use for PAD access. When used with the **x25 pad-access** interface configuration command, the **x25 map pad** command restricts incoming PAD access to those statically mapped hosts.

Examples

The following example configures an X.25 interface to restrict incoming PAD access to the single mapped host. This example requires that both incoming and outgoing PAD access use the network user identification (NUID) user authentication.

```
interface serial 1
 x25 pad-access
 x25 map pad 000000010300 nuid johndoe secret
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.
x25 pad-access	Causes the PAD software to accept PAD connections only from statically mapped X.25 hosts.

x25 map rbp local

To configure a router to establish X.25 circuits in response to incoming TCP connections on a specified TCP port, and to use record boundary preservation (RBP) to transfer data between the TCP session and the corresponding X.25 circuit, use the **x25 map rbp local** command in interface configuration mode. To delete the map, use the **no** form of this command.

x25 map rbp *x121-address* [**cud** *string*] **local port** *port* [**cug** *group-number*] [**packetsize** *in-size out-size*] [**recordsize** *size*] [**reverse**] [**roa** *name*] [**throughput** *in out*] [**transit-delay** *milliseconds*] [**windowsize** *in-size out-size*] **q-bit**

no x25 map rbp *x121-address* [**cud** *string*] **local port** *port*

Syntax Description

x121-address	X.121 address of the remote host.
cud *string*	(Optional) Call user data (CUD) to be included in the X.25 call request, as a hexadecimal string.
port *port*	TCP port number on which the router should listen.
cug *group-number*	(Optional) Closed user group (CUG) number (from 1 to 9999) used for the mapping in an outgoing call.
packetsize *in-size out-size*	(Optional) Proposes maximum input packet size (*in-size*) and maximum output packet size (*out-size*). Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
recordsize *size*	(Optional) Maximum length of a record.
reverse	(Optional) Specifies reverse charging for outgoing calls.
roa *name*	(Optional) Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operating Agencies (ROAs, formerly called Recognized Private Operating Agencies, or RPOAs) to use in outgoing Call Request packets.
throughput *in out*	(Optional) Sets the requested throughput class values for input (*in*) and output (*out*) throughput across the network. Values for *in* and *out* are in bits per second (bps) and range from 75 to 48000 bps.
transit-delay *milliseconds*	(Optional) Transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
windowsize *in-size out-size*	(Optional) Inbound and outbound window sizes (the number of packets permitted in each direction before an acknowledgment is required). Both values typically are the same, must be in the range from 1 to 127, and must be less than the value set by the **x25 modulo** command.
q-bit	(Optional) Supports conveyance of Q-bit data packets between X.25 and TCP/IP hosts.

Defaults

No SVC is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(11)T	The **q-bit** optional keyword was added.

Usage Guidelines

RBP enables X.25 hosts to exchange data with TCP/IP hosts via TCP sessions while maintaining X.25 packet boundaries.

When the **x25 map rbp local** command is configured, the router will listen for a request for a TCP connection to the specified TCP port. When the connection request is accepted, the router will then attempt to place an X.25 call on the interface on which the command was configured, using the X.25 address of the interface as the calling address, the X.121 address specified in the command as the destination address, and the call user data specified in the command. If the call is not successfully completed, the TCP connection will be closed.

The number of connections that may be established to the TCP port is limited only by router resources (such as memory, processor utilization, and available X.25 circuits).

When connections that will be established by the TCP/IP host are configured, the local TCP port number must be unique, with the exception that the same TCP port number may be configured once on each of multiple X.25 interfaces that will not be active simultaneously; this includes the case in which one X.25 interface is configured as a backup interface for another X.25 interface.

No information from the TCP connection is included in the X.25 Call packet sent to the X.25 host.

Examples

In the following example, when the router receives a TCP connection request on port 9999, the host will make an X.25 call to X.121 address 12131 with no call user data.

```
interface Serial1/0
 encapsulation x25 dce
 x25 address 13133
 x25 map rbp 12131 local port 9999
```

Related Commands

Command	Description
show x25 map	Displays information about configured address maps.
show x25 vc	Displays information about active SVCs and PVCs.
x25 map rbp remote	Establishes TCP sessions in response to incoming X.25 calls and uses RBP to transfer data between the X.25 circuit and the corresponding TCP session.
x25 modulo	Sets the window modulus.
x25 pvc rbp local	Accepts an incoming TCP connection and uses RBP to transfer data between the TCP host and an X.25 PVC.
x25 pvc rbp remote	Establishes a TCP session and uses RBP to transfer data between the X.25 host and the TCP session.
x25 roa	Specifies a sequence of packet network carriers.

x25 map rbp remote

To configure a router to establish TCP sessions in response to incoming X.25 calls, and to use record boundary preservation (RBP) to transfer data between the X.25 circuit and the corresponding TCP session, use the **x25 map rbp remote** command in interface configuration mode. To delete the map, use the **no** form of this command.

x25 map rbp *x121-address* [**cud** *string*] **remote host** *ip-address* **port** *port* [**accept-reverse**] [**recordsize** *size*] [**source-interface** *interface*] **q-bit**

no x25 map rbp *x121-address* [**cud** *string*] **remote host port** *port*

Syntax Description

x121-address	X.121 address of the remote host.
cud *string*	(Optional) Call user data (CUD) to be included in the X.25 call request, as a hexadecimal string.
host *ip-address*	Remote IP address for the TCP connection request.
port *port*	Remote TCP port number for the TCP connection request.
accept-reverse	(Optional) Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
recordsize *size*	(Optional) Maximum length of a record.
source-interface *interface*	(Optional) Name of an interface whose IP address will be used as the local IP address for the TCP connection.
q-bit	(Optional) Supports conveyance of Q-bit data packets between X.25 and TCP/IP hosts.

Defaults

No SVC is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(11)T	The **q-bit** optional keyword was added.

Usage Guidelines

RBP enables X.25 hosts to exchange data with TCP/IP hosts via TCP sessions while maintaining X.25 packet boundaries.

The router will accept an incoming X.25 call if the source address and call user data in the call request match the values configured in the **x25 map rbp remote** command. If the **cud** parameter is specified in the command, the call user data in the incoming call must match the configured value exactly. If the **cud** parameter is not specified in the command, the call user data must not conflict with any protocol ID recognized by the router, but it is otherwise ignored.

If an incoming call requests reverse charging, and the accept-reverse option is not specified in the matching map, the call will be refused.

If the incoming call is accepted, the router will attempt to open a TCP connection to a configured IP address and TCP port using a dynamically assigned local TCP port number. If the TCP connection cannot be opened, the X.25 call will be cleared.

The number of X.25 calls that may be accepted is limited only by router resources.

No information from the X.25 call packet is provided to the TCP/IP host.

Examples

In the following example, when serial interface 1/0 receives a call from a remote host that has the X.121 address 12132, the router will open a TCP connection to port number 9999 on the TCP/IP host that has the IP address 10.0.0.1.

```
interface Serial1/0
 encapsulation x25 dce
 x25 address 12030
 x25 map rbp 12132 remote host 10.0.0.1 port 9999
```

Related Commands

Command	Description
show x25 map	Displays information about configured address maps.
show x25 vc	Displays information about active SVCs and PVCs.
x25 map rbp local	Establishes X.25 circuits in response to incoming TCP connections on a specified TCP port, and uses RBP to transfer data between the TCP session and the corresponding X.25 circuit.
x25 pvc rbp local	Accepts incoming TCP connections uses RBP to transfer data between the TCP host and an X.25 PVC.
x25 pvc rbp remote	Establishes TCP sessions and uses RBP to transfer data between the X.25 host and the TCP session.

x25 modulo

To set the window modulus, use the **x25 modulo** interface configuration command.

x25 modulo *modulus*

Syntax Description

modulus	Either 8 or 128. The value of the modulo parameter must agree with that of the device on the other end of the X.25 link.

Defaults

8

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

X.25 supports flow control with a sliding window sequence count. The window counter restarts at zero upon reaching the upper limit, which is called the *window modulus*. Modulo 128 operation is also referred to as *extended packet sequence numbering*, which allows larger packet windows.

Examples

The following example sets the window modulus to 128:

```
interface serial 0
 x25 modulo 128
```

Related Commands

Command	Description
x25 facility	Forces facilities on a per-call basis for calls originated by the router (switched calls are not affected).
x25 win	Changes the default incoming window size to match that of the network.
x25 wout	Changes the default outgoing window size to match that of the network.

x25 nvc

To specify the maximum number of virtual circuits (VCs) that a protocol can have open simultaneously to one host, use the **x25 nvc** command in interface configuration mode. To increase throughput across networks, you can establish up to eight virtual circuits to a host and protocol.

x25 nvc *count*

Syntax Description

count	Circuit count from 1 to 8. A maximum of eight virtual circuits can be configured for each protocol-host pair. Protocols that do not tolerate out-of-sequence delivery, such as encapsulated TCP/IP header compression, will use only one virtual circuit despite this value. Permitting more than one VC may help throughput on slow networks.

Defaults

1

Command Modes

Interface configuration
X.25 profile 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

When the windows and output queues of all existing connections to a host are full, a new virtual circuit will be opened to the designated circuit count. If a new connection cannot be opened, the data is dropped.

Note The *count* value specified for the **x25 nvc** command affects the default value for the number of VCs. It does not affect the **nvc** option for any **x25 map** commands that are configured.

Examples

The following example sets the default maximum number of VCs that each map can have open simultaneously to 4:

```
interface serial 0
 x25 nvc 4
```

x25 ops

To set the interface default maximum output packet size to match that of the network, use the **x25 ops** interface configuration command.

x25 ops *bytes*

Syntax Description

bytes	Byte count that is one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.

Defaults

128 bytes

Command Modes

Interface configuration
X.25 profile 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

X.25 networks use maximum output packet sizes set by the network administrator. Larger packet sizes are better because smaller packets require more overhead processing. To send a packet larger than the X.25 packet size over an X.25 virtual circuit, the Cisco IOS software must break the packet into two or more X.25 packets with the more data bit (M-bit) set. The receiving device collects all packets with the M-bit set and reassembles the original packet.

Note Set the **x25 ips** and **x25 ops** commands to the same value unless your network supports asymmetry between input and output packets.

Examples

The following example sets the default maximum packet sizes to 512:

```
interface serial 1
 x25 ips 512
 x25 ops 512
```

Related Commands

Command	Description
x25 ips	Sets the interface default maximum input packet size to match that of the network.

x25 pad-access

To cause the packet assembler/disassembler (PAD) software to accept PAD connections only from statically mapped X.25 hosts, use the **x25 pad-access** command in interface configuration mode. To disable checking maps on PAD connections, use the **no** form of this command.

x25 pad-access

no x25 pad-access

Syntax Description

This command has no arguments or keywords.

Defaults

Accept PAD connections from any host.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	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

By default, all PAD connection attempts are processed for session creation or protocol translation, subject to the configuration of those functions. If you use the **x25 pad-access** command, PAD connections are processed only for incoming calls with a source address that matches a statically mapped address configured with the **x25 map pad** interface configuration command. PAD connections are refused for any incoming calls with a source address that has not been statically mapped.

Examples

The following example restricts incoming PAD access on the interface to attempts from the host with the X.121 address 000000010300:

```
interface serial 1
 x25 pad-access
 x25 map pad 000000010300
```

Related Commands

Command	Description
service pad	Enables all PAD commands and connections between PAD devices and access servers.
x25 map pad	Configures an X.121 address mapping for PAD access over X.25.

Command	Description
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

x25 profile

To configure an X.25 profile without allocating any hardware specific information, use the **x25 profile** command in global configuration mode. To delete this profile, use the **no** form of this command.

x25 profile *name* {**dce** | **dte** | **dxe**}

no x25 profile *name*

Syntax Description

name	X.25 profile name that you assign.
dce	Specifies a data communications equipment (DCE) interface.
dte	Specifies a data terminal equipment (DTE) interface.
dxe	Specifies a data exchange equipment (DXE) interface.

Defaults

A DCE interface is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(7)T	The **x25 subscribe flow-control** command was added to the X.25 profile configuration mode X.25 options.
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

You can enable many X.25 commands in X.25 profile configuration mode. Table 111 lists the following X.25 commands in X.25 profile configuration mode, which you may use to create your X.25 profile.

Table 111 x25 profile Configuration Mode X.25 Options

Command	Description
x25 accept-reverse	Accepts all reverse charged calls.
x25 address	Sets interface X.121 address.
x25 alias	Defines an alias address pattern.
x25 aodi	Enables AODI (Always On/Direct ISDN) Service.
x25 default	Sets protocol for calls with unknown Call User Data.
x25 facility	Sets explicit facilities for originated calls.
x25 hic	Sets highest incoming channel.

Table 111 x25 profile Configuration Mode X.25 Options (continued)

Command	Description
x25 hoc	Sets highest outgoing channel.
x25 hold-queue	Sets limit on packets queued per circuit.
x25 hold-vc-timer	Sets time to prevent calls to a failed destination.
x25 htc	Sets highest two-way channel.
x25 idle	Sets inactivity time before clearing switched virtual circuit (SVC).
x25 lic	Sets lowest incoming channel.
x25 linkrestart	Restarts when Link Access Procedure, Balanced (LAPB) resets.
x25 loc	Sets lowest outgoing channel.
x25 ltc	Sets lowest two-way channel.
x25 map	Maps protocol addresses to X.121 address.
x25 modulo	Sets operating standard.
x25 nonzero-dte-cause	Allows non-zero DTE cause codes.
x25 nvc	Sets maximum virtual circuits (VCs) simultaneously open to one host per protocol.
x25 ops	Sets default maximum output packet size.
x25 subscribe flow-control	Controls flow control parameter negotiation facilities in call setup packets.
x25 suppress-called-address	Omits destination address in outgoing calls.
x25 suppress-calling-address	Omits source address in outgoing calls.
x25 t10	Sets DCE Restart Request retransmission timer.
x25 t11	Sets DCE Call Request retransmission timer.
x25 t12	Sets DCE Reset Request retransmission timer.
x25 t13	Sets DCE Clear Request retransmission timer.
x25 threshold	Sets packet count acknowledgment threshold.
x25 use-source-address	Uses local source address for forwarded calls.
x25 win	Sets default input window (maximum unacknowledged packets).
x25 wout	Sets default output window (maximum unacknowledged packets).

Table 112 lists LAPB commands in X.25 configuration mode, which you may use to create your X.25 profile.

Table 112 x25 profile lapb Options

Command	Description
interface-outage	Interface outage deadband (partial T3).
k	Maximum number of outstanding frames (window size).
modulo	Set frame numbering modulus.

Table 112 x25 profile lapb Options (continued)

Command	Description
N2	Maximum number of attempts to transmit a frame.
T1	Retransmission timer.
T2	Explicit acknowledge deferral timer.
T4	Keepalive timer.

Examples

The following example shows the NetworkNodeA profile being set as a DCE interface, and with **x25 htc**, **x25 idle**, **x25 accept-reverse**, and **x25 modulo** commands enabled:

```
Router(config)# x25 profile NetworkNodeA dce
Router(config-x25)# x25 htc 128
Router(config-x25)# x25 idle 5
Router(config-x25)# x25 accept-reverse
Router(config-x25)# x25 modulo 128
```

Related Commands

Command	Description
show x25 profile	Displays information about configured X.25 profiles.

x25 pvc (encapsulation)

To establish an encapsulation permanent virtual circuit (PVC), use the encapsulating version of the **x25 pvc** command in interface configuration mode. To delete the PVC, use the **no** form of this command with the appropriate channel number.

x25 pvc *circuit protocol address* [*protocol2 address2* [...[*protocol9 address9*]]] *x121-address* [*option*]

no x25 pvc *circuit*

Syntax Description

circuit	Virtual-circuit channel number, which must be less than the virtual circuits assigned to the switched virtual circuits (SVCs).
protocol	Protocol type, entered by keyword. Supported protocols are listed in Table 113. As many as nine protocol and address pairs can be specified in one command line.
address	Protocol address of the host at the other end of the PVC.
x121-address	X.121 address.
option	(Optional) Provides additional functionality or allows X.25 parameters to be specified for the PVC. Can be any of the options listed in Table 114.

Defaults

The PVC window and maximum packet sizes default to the interface default values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The **apollo**, **vines**, and **xns** arguments were removed because Apollo Domain, 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

PVCs are not supported for ISO Connection-Mode Network Service (CMNS).

You no longer need to specify a datagram protocol-to-address mapping before you can set up a PVC; a map is implied from the PVC configuration. Configurations generated by the router will no longer specify a map for encapsulating PVCs.

When configuring a PVC to carry CLNS traffic, use the X.121 address as the subnetwork point of attachment (SNPA) to associate the PVC with a CLNS neighbor configuration. When configuring a PVC to carry transparent bridge traffic, the X.121 address is required to identify the remote host to the bridging function. Other encapsulation PVCs do not require an X.121 address.

Table 113 lists supported protocols.

Table 113 Protocols Supported by X.25 PVCs

Keyword	Protocol
appletalk	AppleTalk
bridge	Bridging[1]
clns	OSI Connectionless Network Service
compressedtcp	TCP/IP header compression
decnet	DECnet
ip	IP
ipx	Novell IPX
qllc	SNA encapsulation in X.25[2]

1. Bridging traffic is supported only for Cisco's traditional encapsulation method, so a bridge PVC cannot specify other protocols.
2. QLLC is not available for multiprotocol encapsulation.

Table 114 lists supported X.25 PVC options.

Table 114 x25 pvc Options

Option	Description
broadcast	Causes the Cisco IOS software to direct any broadcasts sent through this interface to this PVC. This option also simplifies the configuration of OSPF.
method {**cisco** | **ietf** | **snap** | **multi**}	Specifies the encapsulation method. The choices are as follows: • **cisco**—Single protocol encapsulation; not available if more than one protocol is carried. • **ietf**—Default RFC 1356 operation; single-protocol encapsulation unless more than one protocol is carried, and protocol identification when more than one protocol is carried. • **snap**—RFC 1356 operation where IP is identified when more than one protocol is carried using the SNAP encoding. • **multi**—Multiprotocol encapsulation used on the PVC.
packetsize *in-size out-size*	Maximum input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Both values are typically the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.

Table 114 x25 pvc Options (continued)

Option	Description
passive	Specifies that transmitted TCP datagrams will be compressed only if they were received compressed. This option is available only for PVCs carrying compressed TCP/IP header traffic.
windowsize *in-size out-size*	Packet count for input window (*in-size*) and output window (*out-size*) for the PVC. Both values are typically the same, must be in the range 1 to 127, and must be less than the value set for the **x25 modulo** command.

Examples

The following example establishes a PVC on channel 2 to encapsulate VINES and IP with the far host:

```
interface serial 0
 x25 ltc 5
 x25 pvc 2 vines 60002A2D:0001 ip 172.20.170.91 11110001
```

Related Commands

Command	Description
x25 map	Sets up the LAN protocols-to-remote host mapping.

x25 pvc (switched PVC to SVC)

To configure a switched permanent virtual circuit (PVC) to a switched virtual circuit (SVC) for a given interface, use the switched PVC to SVC version of the **x25 pvc** interface configuration command.

x25 pvc *number1* **svc** *x121-address* [*flow-control-options*] [*call-control-options*]

Syntax Description

number1	Logical channel ID of the PVC. Value must be lower than any range of circuit numbers defined for SVCs.
svc	Specifies a SVC type.
x121-address	Destination X.121 address for opening an outbound SVC and source X.121 address for matching an inbound SVC.
flow-control-options	(Optional) Adds certain features to the mapping specified. It can be any of the options listed in Table 115.
call-control-options	(Optional) Adds certain features to the mapping specified. It can be any of the options listed in Table 116.

Defaults

This command has no default values.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	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 PVC window and maximum packet sizes default to the interface default values. The default idle time comes from the interface on which the **x25 pvc** command is configured, not the interface on which the call is sent/received.

PVC circuit numbers must come before (that is, be numerically smaller than) the circuit numbers allocated to any SVC range.

On an outgoing call, the packet size facilities and window size facilities will be included. The call will be cleared if the call accepted packet specifies different values.

On an incoming call, requested values that do not match the configured values will be refused.

Table 115 lists the flow control options supported by X.25 during PVC to SVC switching.

Table 115 x25 pvc Flow Control Options

Option	Description
packetsize *in-size out-size*	Maximum input packet size (*in-size*) and output packet size (*out-size*) for both the PVC and SVC. Values may differ but must be one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
windowsize *in-size out-size*	Packet count for input window (*in-size*) and output window (*out-size*) for both the PVC and SVC. Both values may differ but must be in the range 1 to 127 and must be less than the value set for the **x25 modulo** command.

Table 116 lists the call control options supported by X.25 during PVC to SVC switching.

Table 116 x25 pvc Call Control Options

Option	Description
accept-reverse	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
idle *minutes*	Idle time-out for the SVC. This option will override the interface's **x25 idle** command value only for this circuit.
no-incoming	Establishes a switched virtual circuit to the specified X.121 address when data is received from the permanent virtual circuit, but does not accept calls from this X.121 address.
no-outgoing	Accepts an incoming call from the specified X.121 address, but does not attempt to place a call when data is received from the permanent virtual circuit. If data is received from the permanent virtual circuit while no call is connected, the PVC will be reset.

Examples

The following example configures PVC to SVC switching between two serial interfaces:

```
x25 routing
interface serial0
 encapsulation x25
 x25 address 201700
 x25 ltc 128
 x25 idle 2
interface serial2
 encapsulation x25 dce
 x25 address 101702

x25 route ^20 interface serial0
x25 route ^10 interface serial2
interface serial0

 x25 pvc 5 svc 101601 packetsize 128 128 windowsize 2 2 no-incoming
 x25 pvc 6 svc 101602 packetsize 128 128 windowsize 2 2 no-outgoing idle 0
 x25 pvc 7 svc 101603 packetsize 128 128 windowsize 2 2
```

Any call with a destination address beginning with 20 will be routed to serial interface 0. Any call with a destination address beginning with 10 will be routed to serial interface 2. (Note that incoming calls will not be routed back to the same interface from which they arrived.)

Traffic received on PVC 5 on serial interface 0 will cause a call to be placed from address 201700 to the X.121 address 101601. The routing table will then forward the call to serial interface 2. If no data is sent or received on the circuit for two minutes, the call will be cleared, as defined by the **x25 idle** command. All incoming calls from 101601 to 201700 will be refused, as defined by the *no-incoming* attribute.

The second **x25 pvc** command configures the circuit to allow incoming calls from 101602 to 201700 to be connected to PVC 6 on serial interface 1. Because idle is set to 0, the call will remain connected until cleared by the remote host or an X.25 restart. Because outgoing calls are not permitted for this connection, if traffic is received on PVC 6 on serial interface 0 before the call is established, the traffic will be discarded and the PVC will be reset.

The last **x25 pvc** command configures the circuit to accept an incoming call from 101603 to 201700 and connects the call to PVC 7 on serial interface 0. If no data is sent or received on the circuit for two minutes, the call will be cleared. If traffic is received on PVC 7 on serial interface 0 before the call is established, a call will be placed to 101503 to 201700.

x25 pvc (switched)

To configure a switched permanent virtual circuit (PVC) for a given interface, use the switched version of the **x25 pvc** interface configuration command.

x25 pvc *number1* **interface** *type number* **pvc** *number2* [*option*]

Syntax Description

number1	PVC number that will be used on the local interface (as defined by the primary interface command).
interface	Required keyword to specify an interface.
type	Remote interface type.
number	Remote interface number.
pvc	Required keyword to specify a switched PVC.
number2	PVC number that will be used on the remote interface.
option	(Optional) Adds certain features to the mapping specified; can be either option listed in Table 117.

Defaults

The PVC window and maximum packet sizes default to the interface default values.

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

You can configure X.25 PVCs in the X.25 switching software. As a result, data terminal equipment (DTE) devices that require permanent circuits can be connected to the router acting as an X.25 switch and have a properly functioning connection. X.25 resets will be sent to indicate when the circuit comes up or goes down.

PVC circuit numbers must come before (that is, be numerically smaller than) the circuit numbers allocated to any SVC range.

Table 117 lists the switched PVC options supported by X.25.

Table 117 x25 pvc Switched PVC Options

Option	Description
packetsize *in-size out-size*	Maximum input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Both values must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
windowsize *in-size out-size*	Packet count for input window (*in-size*) and output window (*out-size*) for the PVC. Both values should be the same, must be in the range 1 to 127, and must not be greater than the value set for the **x25 modulo** command.

Examples

The following example configures a PVC connected between two serial interfaces on the same router. In this type of interconnection configuration, the alternate interface must be specified along with the PVC number on that interface. To make a working PVC connection, two commands must be specified, each pointing to the other, as this example illustrates.

```
interface serial 0
 encapsulation x25
 x25 ltc 5
 x25 pvc 1 interface serial 1 pvc 1
interface serial 1
 encapsulation x25
 x25 ltc 5
 x25 pvc 1 interface serial 0 pvc 1
```

x25 pvc (XOT)

To connect two permanent virtual circuits (PVCs) across a TCP/IP LAN, use the X.25-over-TCP (XOT) service form of the **x25 pvc** command in interface configuration mode.

x25 pvc *number1* **xot** *address* **interface serial** *string* **pvc** *number2* [*option*]

Syntax Description

number1	PVC number of the connecting device.
xot	Indicates two PVCs will be connected across a TCP/IP LAN using XOT.
address	IP address of the device to which you are connecting.
interface serial	Indicates the interface is serial.
string	Serial interface specification that accepts either a number or a string in model 7000 format (*number*/*number*) to denote the serial interface.
pvc	Indicates a PVC.
number2	Remote PVC number on the target interface.
option	(Optional) Adds certain features for the connection; can be one or more of the options listed in Table 118.

Defaults

The PVC window and packet sizes default to the interface default values.

The default for the **xot-keepalive-period** option is 60 seconds.

The default for the **xot-keepalive-tries** option is 4 tries.

Command Modes

Interface 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

Use the PVC tunnel commands to tell the Cisco IOS software what the far end of the PVC is connected to. The incoming and outgoing packet sizes and window sizes must match the remote PVC outgoing and incoming sizes.

It is recommended that the **xot-source** option be used on the remote host so that a consistent IP address is used for the connection.

Table 118 lists the PVC tunnel options supported by X.25.

Table 118 x25 pvc PVC Tunnel Options

Option	Description
packetsize *in-size out-size*	Maximum input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Both values must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
windowsize *in-size out-size*	Packet count for input window (*in-size*) and output window (*out-size*) for the PVC. Both values should be the same, must be in the range 1 to 127, and must not be greater than or equal to the value set for the **x25 modulo** command.
xot-keepalive-period *seconds*	Number of seconds between keepalives for XOT connections. The default is 60 seconds.
xot-keepalive-tries *count*	Number of times TCP keepalives should be sent before dropping the connection. The default value is 4 times.
xot-promiscuous	Indicates that the remote IP address should be ignored when matching an incoming XOT connection with the XOT PVC parameters.
xot-source *interface*	Specifies an interface whose IP address should be used as the local IP address of the TCP connection.

Each XOT connection relies on a TCP session to carry traffic. To ensure that these TCP sessions remain connected in the absence of XOT traffic, use the **service tcp-keepalives-in** and **service tcp-keepalives-out** global configuration commands. If TCP keepalives are not enabled, the XOT PVCs might encounter problems if one end of the connection is reloaded. When the reloaded host attempts to establish a new connection, the other host refuses the new connection because it has not been informed that the old session is no longer active. Recovery from this state requires the other host to be informed that its TCP session is no longer viable so that it attempts to reconnect the PVC.

Also, TCP keepalives inform a router when an XOT switched virtual circuit (SVC) session is not active, thus freeing the router's resources.

Examples

The following example enters the parameters for one side of a connection destined for a platform other than the Cisco 7000 series with RSP7000:

```
service tcp-keepalives-in
service tcp-keepalives-out
interface serial 0
 x25 pvc 1 xot 172.20.1.2 interface serial 1 pvc 2

The following example enters the parameters for one side of a connection destined for the
Cisco 7000 series with RSP7000:
service tcp-keepalives-in
service tcp-keepalives-out
interface serial 0
 x25 pvc 1 xot 172.20.1.2 interface serial 1/1 pvc 2
```

Refer to the section "X.25 and LAPB Configuration Examples" in the *Cisco IOS Wide-Area Networking Configuration Guide* for more complete configuration examples.

Related Commands

Command	Description
service tcp-keepalives-in	Generates keepalive packets on idle incoming network connections (initiated by the remote host).
service tcp-keepalives-out	Generates keepalive packets on idle outgoing network connections (initiated by a user).

x25 pvc rbp local

To configure a router to accept an incoming TCP connection on a specified TCP port, and to use record boundary preservation (RBP) over that session to transfer data between the TCP host and an X.25 permanent virtual circuit (PVC), use the **x25 map rbp local** command in interface configuration mode. To delete the PVC, use the **no** form of this command.

x25 pvc *circuit* **rbp local port** *port* [**packetsize** *in-size out-size*] [**recordsize** *size*] [**windowsize** *in-size out-size*] [**q-bit**]

no x25 pvc *circuit*

Syntax Description[

circuit	Virtual-circuit channel number, which must be less than the virtual circuits assigned to the switched virtual circuits (SVCs).
port *port*	TCP port number on which the router should listen.
packetsize *in-size out-size*	(Optional) Maximum input packet size (*in-size*) and output packet size (*out-size*) for the PVC. The two values are typically the same and must be one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
recordsize *size*	(Optional) Maximum length of a record.
windowsize *in-size out-size*	(Optional) Packet count for input window (*in-size*) and output window (*out-size*) for the PVC. The two values are typically the same, must be in the range from 1 to 127, and must be less than the value set for the **x25 modulo** command.
q-bit	(Optional) Supports conveyance of Q-bit data packets between X.25 and TCP/IP hosts.

Defaults

No PVC is configured.

The PVC window and maximum packet sizes default to the interface default values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(11)T	The **q-bit** optional keyword was added.

Usage Guidelines

RBP enables X.25 hosts to exchange data with TCP/IP hosts via TCP sessions while maintaining X.25 packet boundaries.

When the Q-bit option is included in this command, X.25 Q-bit data packets can be received by the TCP/IP host; otherwise transmission of X.25 Q-bit data packets would bring down the TCP and X.25 sessions.

When connections that will be established by the TCP/IP host are configured, the local TCP port number must be unique, with the exception that the same TCP port number may be configured once on each of multiple X.25 interfaces that will not be active simultaneously. This includes situations in which one X.25 interface is configured as a backup interface for another X.25 interface.

When the **x25 pvc rbp local** command is configured, the router will listen for a TCP connection request to the configured TCP port. Until the connection request is received, the router will acknowledge any X.25 reset packets on the circuit. When the TCP connection request is received, the connection will be accepted, and the router will send an X.25 reset packet over the configured X.25 destination circuit. If the reset packet is not acknowledged, the TCP connection will be closed.

Since this command is associated with a specific X.25 circuit, only one connection may be active per command.

When a PVC is configured, the virtual circuit must be unique. Multiple commands referencing the same virtual circuit (matching logical channel identifier and interface) are not permitted.

When connections that will be established by the TCP/IP host are configured, the local TCP port number must be unique, with the exception that the same TCP port number may be configured once on each of multiple X.25 interfaces that will not be active simultaneously. This includes the case in which one X.25 interface is configured as a backup interface for another X.25 interface.

Examples

The following example shows the configuration of a PVC with RBP. In this example, the router will listen for a TCP connection request on port 9999. When a TCP connection is established, the router will send an X.25 reset over the configured X.25 destination circuit.

```
Interface serial2/1
 encapsulation x25
 x25 pvc 2 rbp local port 9999
```

Related Commands

Command	Description
show x25 map	Displays information about configured address maps.
show x25 vc	Displays information about active SVCs and PVCs.
x25 map rbp local	Establishes X.25 circuits in response to incoming TCP connections and uses RBP to transfer data between the TCP session and the X.25 circuit.
x25 map rbp remote	Establishes TCP sessions in response to incoming X.25 calls and uses RBP to transfer data between the X.25 circuit and the TCP session.
x25 pvc rbp remote	Establishes TCP sessions in response to incoming data on an X.25 PVC, and uses RBP to transfer data between the X.25 host and the TCP session.

x25 pvc rbp remote

To configure a router to establish a TCP session in response to data received on an X.25 permanent virtual circuit (PVC) and to use record boundary preservation (RBP) to transfer data between the X.25 host and the TCP session, use the **x25 pvc rbp remote** command in interface configuration mode. To delete the PVC, use the **no** form of this command.

x25 pvc *circuit* **rbp remote host** *ip-address* **port** *port* [**packetsize** *in-size out-size*] [**source-interface** *interface*] [**recordsize** *size*] [**windowsize** *in-size out-size*] **q-bit**

no x25 pvc *circuit*

Syntax Description

circuit	Virtual-circuit channel number, which must be less than the virtual circuits assigned to the switched virtual circuits (SVCs).
host *ip-address*	Remote IP address for the TCP connection.
port *port*	TCP port number on which the router should listen.
packetsize *in-size out-size*	(Optional) Maximum input packet size (*in-size*) and output packet size (*out-size*) for the PVC. The two values are typically the same and must be one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
source-interface *interface*	(Optional) Name of an interface whose IP address will be used as the local IP address for the TCP connection.
recordsize *size*	(Optional) Maximum length of a record.
windowsize *in-size out-size*	(Optional) Packet count for input window (*in-size*) and output window (*out-size*) for the PVC. The two values are typically the same, must be in the range from 1 to 127, and must be less than the value set for the **x25 modulo** command.
q-bit	(Optional) Supports conveyance of Q-bit data packets between X.25 and TCP/IP hosts.

Defaults

The PVC window and maximum packet sizes default to the interface default values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(11)T	The **q-bit** optional keyword was added.

Usage Guidelines

RBP enables X.25 hosts to exchange data with TCP/IP hosts via TCP sessions while maintaining X.25 packet boundaries.

When a PVC is configured, the virtual circuit must be unique. Multiple commands referencing the same virtual circuit (matching logical channel identifier and interface) are not permitted.

When the **x25 pvc rbp remote** command is configured, the router will wait until a data packet is received on a specific X.25 PVC. Until it receives a data packet, the router will acknowledge any X.25 reset packets on the circuit. When a data packet is received, the router will attempt to establish a TCP connection to a configured IP address and TCP port, using a dynamically assigned local TCP port number. If the connection attempt fails, the router will reset the PVC and wait for another data packet before reattempting to establish the TCP connection.

Since the **x25 pvc rbp remote** command is associated with a specific X.25 circuit, at most one connection may be active per command.

Examples

The following example shows an X.25 host configured to use a PVC with RBP. When PVC 1 receives a data packet, the router will attempt to establish a TCP connection to port 9999 at the TCP/IP host that has the IP address 10.0.0.1.

```
interface serial1/0
 encapsulation x25
 x25 pvc 1 rbp remote host 10.0.0.1 port 9999
```

Related Commands

Command	Description
show x25 map	Displays information about configured address maps.
show x25 vc	Displays information about active SVCs and PVCs.
x25 map rbp local	Establishes X.25 circuits in response to incoming TCP connections on a specified TCP port, and uses RBP to transfer data between the TCP session and the X.25 circuit.
x25 map rbp remote	Establishes TCP sessions in response to incoming X.25 calls and uses RBP to transfer data between the X.25 circuit and the TCP session.
x25 pvc rbp local	Accepts incoming TCP connections on a specified TCP port, and uses RBP to transfer data between the TCP host and an X.25 PVC.

x25 relay-vc-number

To enable the relay of a virtual circuit (VC) number for switched calls between X.25 over TCP (XOT) and the interface on which the command is configured, use the **x25 relay-vc-number** command in interface configuration or X.25 profile configuration mode. To disable the relay of the VC number, use the **no** form of this command.

x25 relay-vc-number

no x25 relay-vc-number

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)
X.25 profile configuration (config-x25)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **x25 relay-vc-number** command to enable the relay of the VC number for the switched calls between the XOT and the configured interface.

X.25 is a method of packet switching that is used for communication between user devices (such as routers, bridges, and host machines) and network devices (such as switching nodes and modems). User devices are called data terminal equipment (DTE), and network devices are called data circuit-terminating equipment (DCE).

Examples

The following examples show how to set the **x25 relay-vc-number** command for a Fast Ethernet interface and a serial interface.

```
Router(config)# interface fastethernet0/0
Router(config-if)# cmns enable
Router(config-if)# x25 relay-vc-number

Router(config)# interface serial1/0
Router(config-if)# x25 relay-vc-number
```

Related Commands

Command	Description
cmns enable	Enables the Connection-Mode Network Service (CMNS) on a nonserial interface.

x25 remote-red

Note Effective with Cisco IOS Release 12.2, the **x25 remote-red** command is not available in Cisco IOS Software.

To set up the table that lists the Blacker Front End (BFE) nodes (host or gateways) to which the router will send packets, use the **x25 remote-red** command in interface configuration mode.

x25 remote-red *host-ip-address* **remote-black** *blacker-ip-address*

Syntax Description

host-ip-address	IP address of the host or router that the packets are being sent to.
remote-black	Delimits the addresses for the table being built.
blacker-ip-address	IP address of the remote BFE device in front of the host to which the packet is being sent.

Defaults

No table is set up.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The table that results from this command provides the address translation information that the router sends to the BFE when it is in emergency mode.

Examples

The following example sets up a short table of BFE nodes for serial interface 0:

```
interface serial 0
 x25 remote-red 172.20.9.3 remote-black 172.20.9.13
 x25 remote-red 192.108.15.1 remote-black 192.108.15.26
```

Related Commands

Command	Description
show x25 remote-red	Displays the one-to-one mapping of the host IP addresses and the IP addresses of a remote BFE device.
x25 bfe-decision	Specifies how a router configured for X.25 BFE emergency decision will participate in emergency mode.

x25 retry

To activate a secondary route while also retrying a failed primary route, use the **x25 retry** interface configuration command in conjunction with the ip route or backup interface commands. To discontinue implementing secondary X.25 routes and retrying of primary X.25 routes, use the **no** form of this command.

x25 retry interval *seconds* **attempts** *count*

no x25 retry interval *seconds* **attempts** *count*

Syntax Description

interval	Keyword defining interval between attempts.
seconds	Number of seconds between attempts.
attempts	Keyword defining number of attempts.
count	Number of attempts to reestablish the closed link before discontinuing.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)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

The **x25 retry** command is triggered when no switched virtual circuits (SVCs) are up, and an outgoing call fails.

The retry attempts will continue until any of the following happens:

- The configured retry attempts limit is reached.
- The attempt to reestablish the link is successful.
- An incoming call is received on the subinterface.
- The X.25 packet layer on the interface is restarted.

If the number of retry attempts exceeds the configured limit, the interface will remain marked “down” until any of the following happens:

- An incoming call is received on the subinterface.
- The X.25 packet layer on the interface is restarted.

Examples

The following example shows the **x25 retry** command being configured on subinterface 1.1 with a retry interval of 60 seconds up to a maximum of 10 attempts:

```
Router(config)# interface serial1.1 point-to-point
Router(config-if)# x25 retry interval 60 attempts 10
```

Related Commands

Command	Description
backup interface	Configures an interface as a secondary or dial backup interface.
clear x25	Restarts an X.25 or CMNS service, clears an SVC, or resets a PVC.
ip route	Establishes static routes and defines the next hop for large-scale dialout.

x25 roa

To specify a sequence of packet network carriers, use the **x25 roa** command in global configuration mode. To remove the specified name, use the **no** form of this command.

x25 roa *name number*

no x25 roa *name*

Syntax Description

name	Recognized Operating Agency (ROA, formerly called a Recognized Private Operating Agency, or RPOA), which must be unique with respect to all other ROA names. It is used in the **x25 facility** and **x25 map** interface configuration commands.
number	A sequence of 1 or more numbers used to describe an ROA; up to 10 numbers are accepted.

Defaults

No packet network carriers are specified.

Command Modes

Global 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

This command specifies a list of transit ROAs to use, referenced by name.

Examples

The following example sets an ROA name and then sends the list via the X.25 user facilities:

```
x25 roa green_list 23 35 36
interface serial 0
 x25 facility roa green_list
 x25 map ip 172.20.170.26 10 roa green_list
```

Related Commands

Command	Description
x25 facility	Forces facilities on a per-call basis for calls originated by the router (switched calls are not affected).
x25 map	Sets up the LAN protocols-to-remote host mapping.

x25 rotary

To assign an X.121 address to a rotary group (and optionally, to specify that address to be the source address of calls originating from lines within the group), use the **x25 rotary** command in global configuration mode. To remove an X.121 address from a rotary group, use the **no** form of this command.

x25 rotary *group-num x121-address* [**calling-address** [**rotary** | **line**]

no x25 rotary *group-num x121-address* [**calling-address** [**rotary** | **line**]

Syntax Description

group-num	A number from 1 through 127, assigned to identify the rotary group.
x121-address	X.121 address. The address must be a numerical string no longer than 20 digits.
calling-address	(Optional) The source address of outgoing calls from members of this group. The default calling address is each line's X.121 address.
rotary	Makes the rotary's X.121 address the source address of outgoing calls.
line	Uses each line's absolute address as the source address of outgoing calls.

Command Default

No group X.121 address is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YN	This command was introduced.
12.4(4)T	This command was integrated into Cisco IOS 12.4(4)T.

Usage Guidelines

Each X.121 address can be associated with only one rotary group.

A rotary group cannot be configured with an X.121 address if it has "queued" or "queued-by-role" selection type.

Examples

The following example sets the rotary address to be used as the calling address:

```
Router(config)# x25 rotary 1 1111 calling-address rotary
```

Related Commands

Command	Description
rotary	Defines a group of lines as a rotary ("hunt") group, and optionally, configures their response to connection requests.

x25 route

To create an entry in the X.25 routing table (to be consulted for forwarding incoming calls and for placing outgoing packet assembler/disassembler (PAD) or protocol translation calls), use the **x25 route** command in global configuration mode. To remove an entry from the table, use the **no** form of the command.

x25 route [*#position*] [*selection-options*] [*modification-options*] *disposition-options* [*xot-keepalive-options*]

no x25 route [*#position*] [*selection-options*] [*modification-options*] *disposition-options* [*xot-keepalive-options*]

Syntax Description

#position	(Optional) A pound sign (#) followed by a number designates the position in the routing table at which to insert the new entry. If no value for the *position* argument is given, the entry is appended to the end of the routing table.
selection-options	(Optional) The selection options identify when the subsequent modification and disposition options apply to an X.25 call; any or all variables may be specified for a route. For selection keyword and argument options, see Table 119 in the "Usage Guidelines" section. For selection and modification pattern and character matching and replacement see Table 121, Table 122, and Table 123 in the "Usage Guidelines" section. Although each individual selection criterion is optional, at least one selection or modification option must be specified in the **x25 route** command.
modification-options	(Optional) The modification options modify the source or destination addresses of the selected calls. The standard regular expression substitution rules are used, where a match pattern and rewrite string direct the construction of a new string. For modification keyword and argument options, see Table 120 in the "Usage Guidelines" section. For selection and modification pattern and character matching and replacement see Table 121, Table 122, and Table 123 in the "Usage Guidelines" section. Although each individual modification is optional, at least one selection or modification option must be specified in the **x25 route** command.
disposition-options	Specifies the disposition of a call matching the specified selection pattern. For disposition keyword and argument options, see Table 124 in the "Usage Guidelines" section.
xot-keepalive-options	(Optional) The XOT-keepalive options specify an X.25 over TCP (XOT) keepalive period and number of XOT-keepalive retries. XOT relies on TCP to detect when the underlying connection is dead. TCP detects a dead connection when sent data goes unacknowledged for a given number of attempts over a period of time. For XOT-keepalive keyword and argument options, see Table 125 in the "Usage Guidelines" section.

Defaults

No entry is created in the X.25 routing table.

Command Modes Global configuration

Command History

Release	Modification
11.3	The following modifications were made: • The selection option keywords **source** and **dest-ext** and the interface *disposition* to a Connection-Mode Network Service (CMNS) destination was added. In prior releases, CMNS routing information was implied by maps defining a network service access point (NSAP) prefix for a CMNS host's MAC address. • The **clear interface** *disposition option* was added. In prior releases, the disposition was implicit in a route to the Null 0 interface.
12.0(3)T	The interface-based calling address insertion and removal feature was introduced.
12.0(5)T	The following modifications were made: • For the DNS-Based X.25 Routing feature, the **dns** keyword and *pattern* argument (see Table 123) were added. • The enhanced **x25 route** command replaces the **x25 map cmns** command. The **x25 route alias** form of this command (supported in earlier releases) was replaced by the **x25 alias** command.
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 enhanced **x25 route** command replaces the **x25 map cmns** command. The **x25 route alias** form of this command (supported in earlier releases) has been replaced by the **x25 alias** command.

The modification options are long-standing but newly applicable to all dispositions in Cisco IOS Release 11.3 and later.

Note The entire command must be entered on one line.

Selection Options

Selection arguments specify match criteria. When a call matches all selection criteria in an X.25 route, then the specified modification and disposition are used for the call.

As many as four selection options can be used to determine the route:

- Called X.121 network interface address (destination or source host address)
- Called address extension (destination NSAP address)
- X.25 packet's call user data (CUD) field
- Input interface from which the call was received (**input-interface** option)

Table 119 lists the selection options for the **x25 route** command. At least one selection or modification option must be specified.

Table 119 x25 route Selection Options

Selection Option	Description
cud *user-data-pattern*	(Optional) CUD pattern, which is specified as a regular expression of printable ASCII text. The CUD field may be present in a call packet. The first few bytes (commonly 4 bytes long) identify a protocol; the specified pattern is applied to any user data after the protocol identification.
destination-pattern	(Optional) Destination address pattern, which is a regular expression that can represent either one X.121 address (such as ^1111000$) or any address in a group of X.121 addresses (such as ^1111.*).
dest-ext *nsap-destination-pattern*	(Optional) NSAP destination address pattern, which is a regular expression that can represent either an NSAP destination address (such as ^11.1111.0000$) or an NSAP prefix (such as ^11.1111.*). **Note** A period (.) in the pattern is interpreted as a character wildcard, which will not interfere with a match to the actual period in the NSAP; if desired, an explicit character match may be used (such as ^11\.1111\..*).
hunt-group *name*	Routes the selected call to the X.25 hunt group. The chosen router may vary depending on the hunt group configuration.
input interface *interface number*	(Optional) Specifies interface number on which the call will be received.
source *source-pattern*	(Optional) Source address pattern, which is a regular expression that can represent either one X.121 source address (such as ^2222000$) or any address in a group of X.121 addresses (such as ^2222.*).

Note The X.121 and NSAP addresses are specified as regular expressions. A common error is to specify the address digits without anchoring them to the beginning and end of the address. For example, the regular expression 1111 will match an X.121 address that has four successive 1s somewhere in the address; to specify the single X.121 address, the form ^1111$ must be used.

Regular expressions are used to allow pattern-matching operations on the addresses and user data. A common operation is to use prefix matching on the X.121 Data Network Identification Code (DNIC) field and route accordingly. The caret (^) is a special regular expression character that anchors the match at the beginning of the pattern. For example, the pattern ^3306 will match all X.121 addresses with a DNIC of 3306.

Modification Options

Addresses typically need to be modified when traffic from a private network that uses arbitrary X.121 addresses must transit a public data network, which must use its own X.121 addresses. The easiest way to meet the requirement is to specify in the **x25 route** command a way to modify the private address into a network X.121 address, or to modify a network X.121 address into a private address. The addresses are modified so that no change to the private addressing scheme is required.

The modification options use the standard UNIX regular expression substitution operations to change an X.25 field. A pattern match is applied to an address field, which is rewritten as directed by a rewrite pattern.

Table 120 lists the modification options for the **x25 route** command. At least one selection or modification option must be specified.

Table 120 x25 route Modification Options

Modification Option	Description
substitute-dest *rewrite-dest*	(Optional) Called X.121 address rewrite pattern. The destination address, *destination-pattern*, and this *rewrite-dest* pattern are used to form a new destination address. If no *destination-pattern* is specified, a default match pattern of .* is used. See Table 121 and Table 122 for summaries of pattern and character matching, respectively. See Table 123 for a summary of pattern rewrite elements.
substitute-source *rewrite-source*	(Optional) Calling X.121 address rewrite pattern. The *source address*, *source-pattern*, and this *rewrite-source* pattern are used to form a new source address. If no *source-pattern* is specified, any *destination-pattern* match pattern is used. If neither match pattern is specified, a default match pattern of .* is used. See Table 121 and Table 122 for summaries of pattern and character matching, respectively. See Table 123 for a summary of pattern rewrite elements.

Note As of Cisco IOS Release 11.3, the **substitute-source** and **substitute-dest** options also apply to PAD calls.

A modification of the source address is directed by the rewrite string using one of three possible match patterns. If the **source** *source-pattern* selection option is defined, it is used with the *source-rewrite* string to construct the new source address; otherwise, a *destination-pattern* regular expression is used (for backward compatibility) or a wildcard regular expression (.*) is used. In the *rewrite-source* argument, the backslash character (\) indicates that the digit immediately following the argument selects a portion of the matched address to be inserted into the new called address.

A modification of the destination address is directed by the rewrite string using one of two possible match patterns. If the *destination-pattern* selection option is defined, it is used with the *destination-rewrite* string to construct the new destination address; otherwise, a wildcard regular

expression (.*) is used. In the *rewrite-dest* argument, the backslash character (\) indicates that the digit immediately following the argument selects a portion of the original called address to be inserted into the new called address.

Pattern and Character Matching and Replacement for Selection and Modification Options

See Table 121, Table 122, and Table 123, respectively, for summaries of pattern matching, character matching, and pattern replacement elements. Note that up to nine pairs of parentheses can be used to identify patterns to be included in the modified string. A more complete description of the pattern-matching characters is found in the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide*.

Table 121 Pattern Matching for x25 route Selection and Modification Options

Pattern	Description
*	Matches 0 or more occurrences of the preceding character.
+	Matches 1 or more occurrences of the preceding character.
?	Matches 0 or 1 occurrences of the preceding character.[1]

1. Precede the question mark with **Ctrl-V** to prevent the question mark from being interpreted as a **help** command.

Table 122 Character Matching for x25 route Selection and Modification Options

Character	Description
^	Matches the beginning of the input string.
$	Matches the end of the input string.
char	Matches the single character *char* specified.
.	Matches any single character.

Table 123 Pattern Replacements for x25 route Selection and Modification Options

Pattern	Description
\0	The pattern is replaced by the entire original address.
\1...9	The pattern is replaced by strings that match the first through ninth parenthetical part of the X.121 address.

Disposition Option

The **xot-source** disposition option can improve the resilience of the TCP connection if, for instance, a loopback interface is specified. By default, a TCP connection's source IP address is that of the interface used to initiate the connection; a TCP connection will fail if either the source or destination IP address is no longer valid. Because a loopback interface never goes down, its IP address is always valid. Any TCP connections originated using a loopback interface can be maintained as long as a path exists to the destination IP address, which may also be the IP address of a loopback interface.

Using the **continue** keyword provides flexibility by reducing the number of X.25 route configurations necessary in the route table by breaking them into separate, simpler, and more manageable tasks. It allows the **x25 route** command to cumulatively hold all specified route entries and carry whatever

selection or modification options you may have just specified on the command line. The route table lookup terminates when a matching route is found among the remaining entries in the route table. The **continue** disposition must be the last option on the **x25 route** command line.

Table 124 lists the disposition options for the **x25 route** command. You must select one of these options.

Table 124 x25 route Disposition Options

Disposition Option	Description
clear	Terminates the call.
continue	(Optional) Combines sequential route table lookups, holding onto any "selections" and "modifications" specified on the **x25 route** statement.
hunt-group *name*	Routes the selected call to the X.25 hunt group. The chosen route may vary depending on the hunt group configuration.
interface *interface number*	Routes the selected call to the specified X.25 serial interface.
interface *interface number* **dlci** *number*	(Optional) Routes the X.25 call to the specified Annex G link. You must include the interface number and enter the data link connection identifier (DLCI) number. You only need to do this if you want the router to accept switched calls, as well as originate them.
interface *cmns-interface* **mac** *mac-address*	Routes the selected call out the specified broadcast interface via CMNS to the LAN destination station. The broadcast interface type can be Ethernet, Token Ring, or FDDI. The interface numbering scheme depends on the router interface hardware.
xot *ip-address* [*ip2-address* [...[*ip6-address*]]] [**xot-source** *interface*]	Routes the selected call to the XOT host at the specified IP address. Subsequent IP addresses are tried, in sequence, only if XOT is unable to establish a TCP connection with a prior address.
xot dns *pattern*	Used with DNS-based X.25 routing, this option consults the DNS to get up to six destination IP addresses using whatever lookup pattern you choose (see Table 123).

XOT-Keepalive Options

TCP maintains each connection using a keepalive mechanism that starts with a default time period and number of retry attempts. If a received XOT connection is dispatched using a route with explicit keepalive parameters, those values will be used for the TCP connection. If an XOT connection is sent using a route with explicit keepalive parameters, those values will be used for the TCP connection.

Table 125 lists and describes the xot-keepalive options for the **x25 route** command.

Table 125 x25 route XOT-Keepalive Options

XOT-Keepalive Option	Description
xot-keepalive-period *seconds*	Number of seconds between keepalives for XOT connections. The default is 60 seconds.
xot-keepalive-tries *count*	Number of times TCP keepalives should be sent before dropping the connection. The default value is 4 times.

X.25 Routing Action When a Match Is Found

If a matching route is found, the incoming call is forwarded to the next hop depending on the routing entry. If no match is found, the call is cleared. If the route specifies a serial interface running X.25 or a broadcast interface running CMNS, the router attempts to forward the call to that host. If the interface is not operational, the subsequent routes are checked for forwarding to an operational interface. If the interface is operational but out of available virtual circuits, the call is cleared. Otherwise, the expected Clear Request or Call Accepted packet is forwarded back toward the originator. A call cannot be forwarded out the interface on which it arrived.

If the matching route specifies an XOT disposition, a TCP connection is established to port 1998 at the specified IP address, which must be an XOT host. The Call Request packet is forwarded to the remote host, which applies its own criteria to handle the call. If, upon receiving an XOT call on the remote host, a routing table entry is not present, or the destination is unavailable, a Clear Request is sent back and the TCP connection is closed. Otherwise, the call is handled and the expected Clear Request or Call Accepted packet is returned. Incoming calls received via XOT connections that match a routing entry specifying an XOT destination are cleared. This restriction prevents Cisco routers from establishing an XOT connection to another router that would establish yet another XOT connection.

X.25 Routing Action When No Match Is Found

If no match is found, the action taken is specific to the application. X.25 switching will clear the call if there is no match in the routing table. X.25 PAD and PAD-related applications, such as protocol translation using X.25, will route the call to the default X.25 interface, which is the first X.25 interface configured.

Examples

The following example uses regular expression pattern matching characters to match just the initial portion of the complete X.25 address. Any call with a destination address beginning with 3107 that is received on an interface other than serial 0 is forwarded to serial 0.

```
x25 route ^3107 interface serial 0
```

The following Annex G example routes the X.25 call to the specified Annex G DLCI link. You must include both interface number and DLCI number. It is this combination of both these numbers that indicates the logical X.25 interface over Frame Relay.

```
x25 route ^2222 interface serial 1 dlci 20
```

The following example prevents X.25 routing for calls that do not specify a source address:

```
x25 route source ^$ clear
```

The following example configures alternate XOT hosts for the routing entry. If the first address listed is not available, subsequent addresses are tried until a connection is made. If no connection can be formed, the call is cleared.

```
x25 route ^3106$ xot 172.20.2.5 172.20.7.10 172.10.7.9
```

The following example clears calls that contain a 3 in the source address. The disposition keyword **clear** is new.

```
x25 route source 3 clear
```

The following example clears calls that contain 33 in the source address:

```
x25 route source 33 clear
```

The following example clears a call to the destination address 9999:

```
x25 route ^9999$ clear
```

The following example specifies a route for specific source and destination addresses. (The ability to combine source and destination patterns is a new feature.)

```
x25 route ^9999$ source ^333$ interface serial 0
```

The following example routes the call to the XOT host at the specified IP address. The disposition keyword **xot** is new. In prior releases the keyword **ip** was used.

```
x25 route ^3333$ xot 172.21.53.61
```

The following DNS-based X.25 routing example shows an X.25 request to the DNS. The **\0** pattern indicates that the entire incoming X.121 address is being used as the index into the DNS, which will return the required IP address.

```
x25 route ^.* xot dns \0
```

The following example routes calls containing the destination extension address preamble 11.1234:

```
x25 route dest-ext ^11.1234.* interface serial 0
```

The following example rewrites the destination address as 9999. There must be a minimum of four 8s in the address. (8888888 will change to 9999.)

```
x25 route 8888 substitute-dest 9999 interface serial 0
```

The following example substitutes only part of the destination address. “^88” specifies the original destination string must begin with 88. “(.*)” indicates the string can end with any number, 0-9, and can be more than one digit. “99\1” changes the destination address to 99 plus whatever matches “.*” in the original destination address. For example, 8881 will change to 9981.

```
x25 route ^88(.*) substitute-dest 99\1 interface serial 0
```

The following example substitutes only part of the destination address and also removes a specified number of digits from the address. “^88” specifies the original destination string must begin with 88. “(..)” matches any two digits. “(.*)” specifies the string can end with any number, 0-9, and can occur zero or more times. Thus any address that starts with 88 and has four or more digits will be rewritten to start with 99 and omit the third and fourth digits. For example, 881234 will change to 9934.

```
x25 route ^88(..)(.*) substitute-dest 99\2 interface serial 0
```

The following example looks for a specified destination address and changes the source address. “9999” is the destination address. The original source address changes to “2222” because the call is made to the destination 9999.

```
x25 route ^9999$ substitute-source 2222 interface serial 0
```

The following example shows insertions and removals in the X.121 address as calls from the X.25 network get routed to X.25 devices. For a call coming from interface serial 0 with a called address starting with 2, the 2 is stripped off the called address and the call forwarded to serial interface 2. For a call coming from interface serial 2 with any calling address, a 2 will be inserted to its calling address and the call forwarded to serial interface 0.

```
x25 route ^02(.*) input-interface serial0 substitute-dest \1 interface serial2
x25 route input-interface serial2 source .* substitute-source 2\0 interface serial0
```

The following example shows how to insert the X.121 address to forward calls among local X.25 devices. For a call on interface 1 with a called address of 0255 and any calling address, the call is forwarded to serial interface 2 with a called address of 55 and a calling address inserted with 01. The **continue** keyword continues address substitution without address forwarding.

```
x25 route input-interface serial1 source .* substitute-source 01\0 continue
x25 route input-interface serial2 source .* substitute-source 02\0 continue
x25 route ^01(.*) substitute-dest \1 interface serial1
x25 route ^02(.*) substitute-dest \1 interface serial2
```

The following example rewrites the source address based on the source address. “9999” matches any destination address with four consecutive 9s. “^...(.*)” matches any source address with at least three digits; the command removes the first three digits and rewrites any digits after the first three as the new source address. For example, a call to 9999 from the source address 77721 will be forwarded using the calling address 21 and the called address 9999.

```
x25 route 9999 source ^...(.*) substitute-source \1 interface serial 0
```

The following example adds a digit to the source and destination addresses patterns. “09990” is the destination address pattern. The source can be any address. “9\0” specifies to add a leading 9 to the destination address pattern. “3\0” specifies to add a leading 3 to the source address pattern. For example, a call using source 03330 and destination 09990 will change to 303330 and 909990, respectively.

```
x25 route 09990 source .* substitute-dest 9\0 substitute-source 3\0 interface serial 0
```

Related Commands

Command	Description
show x25 route	Displays the X.25 routing table.

x25 routing

To enable X.25 switching or tunneling, use the **x25 routing** command in global configuration mode. To disable the forwarding of X.25 calls, use the **no** form of this command.

x25 routing [**acknowledge local** | **acknowledge end-to-end**] [**tcp-use-if-defs**]

no x25 routing [**acknowledge local** | **acknowledge end-to-end**] [**tcp-use-if-defs**]

Syntax Description

acknowledge local	(Optional) Sets local acknowledgment on the router.
acknowledge end-to-end	(Optional) Sets end-to-end acknowledgment. (Default acknowledge setting.)
tcp-use-if-defs	(Optional) Accepts calls received over TCP.

Defaults

This command has no default values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The following keywords were added: • **acknowledge end-to-end** • **acknowledge local**
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 **x25 routing** command enables X.25 switching between the X.25 services (X.25, Connection-Mode Network Service [CMNS] and X.25 over TCP [XOT], and Annex G). X.25 calls will not be forwarded until this command is issued.

The **acknowledge local** and **acknowledge end-to-end** keywords are optional, with **acknowledge end-to-end** being the default. To confirm what type of acknowledgment has been set, use the **show protocol** command.

The **tcp-use-if-defs** keyword may be needed for receiving XOT calls from routers using older software versions. Normally, calls received over a TCP connection (remote routing reception) will have the flow control parameters (window sizes and maximum packet sizes) indicated, because proper operation of routed X.25 requires that these values match at both ends of the connection.

Some previous versions of Cisco IOS software, however, do not ensure that these values are present in all calls. In this case, the Cisco IOS software normally forces universally acceptable flow control values (window sizes of 2 and maximum packet sizes of 128) on the connection. Because some equipment disallows modification of the flow control values in the call confirm, the **tcp-use-if-defs** keyword causes the router to use the default flow control values of the outgoing interface and indicate the resulting values in the call confirm. This modified behavior may allow easier migration to newer versions of the Cisco IOS software.

Examples

The following example enables X.25 routing:

```
x25 routing
```

The following example enables X.25 routing with local acknowledgment:

```
x25 routing acknowledge local
```

x25 security call-conf address out

To suppress the addresses in transmitted X.25 Call Confirm packets or to specify that the addresses originally received in a Call packet are to be encoded in the Call Confirm packet, use the **no x25 security call-conf address out** command in interface configuration or X.25 profile configuration mode. To reenable standard X.25 procedure for handling addresses in Call Confirm packets, use the **x25 security call-conf address out** command.

x25 security call-conf address out

no x25 security call-conf address out source {**suppress** | **unmodified**} **dest** {**suppress** | **unmodified**}

Syntax Description

source	X.121 source address in the Call Confirm packet.
suppress	Suppress the address in the Call Confirm packet.
unmodified	Use the original address that was presented in the Call packet in the Call Confirm packet.
dest	X.121 destination address in the Call Confirm packet.

Defaults

Addresses presented in X.25 Call Confirm packets are determined according to X.25 protocol standards.

Command Modes

Interface configuration
X.25 profile configuration

Command History

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

Usage Guidelines

Network devices that implement nonstandard X.25 service may have special requirements for address encoding in Call Confirm packets. The **no x25 security call-conf address out** command enables you to control the source and destination addresses that are encoded in outgoing Call Confirm packets. You can suppress the addresses completely, or you can specify that the addresses originally presented in the received Call packet be encoded unmodified in the Call Confirm packet.

Caution X.25 specifies address signaling behavior as a security measure to ensure that connecting devices are given clear notice of a call setup that encountered redirection, deflection, or distribution to an alternate destination. Disabling these security features should be done only when the risks of doing so are understood and acceptable.

When address suppression is configured, any address block in the Call Confirm packet will specify the null address (zero digits) for the suppressed addresses.

X.25 Call Confirm address control can be configured on a main interface or an X.25 profile. When this functionality is configured on an interface, all Call Confirm packets sent over the services that use that interface will be affected, including SVCs that use a configuration from a subinterface. When this functionality is configured on an X.25 profile, all services using that profile will be affected.

Examples

The following example shows how to suppress both the source and destination addresses in Call Confirm packets:

```
interface serial 0
 no ip address
 encapsulation x25
 no x25 security call-conf address out source suppress dest suppress
```

Related Commands

Command	Description
debug x25	Displays information about X.25 traffic.
x25 security clamn	Disables the CLAMN security signaling facility in X.25 Call Confirm packets.
x25 security crcdn	Disables the CRCDN security signaling facility in X.25 Call packets.

x25 security clamn

To reenable the Called Line Address Modified Notification (CLAMN) security signaling facility when it has been disabled, use the **x25 security clamn** command in interface configuration mode. To disable the (CLAMN) security signaling facility in X.25 Call Confirm packets, use the **no** form of this command.

x25 security clamn

no x25 security clamn

Syntax Description

This command has no arguments or keywords.

Defaults

The X.25 CLAMN security signaling facility is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The X.25-class services use the CLAMN security signaling facility in X.25 Call Confirm packets to notify the originator of the Call that a security event occurred during X.25 Call setup. The encoding of this facility specifies the reason for the signal, and the X.25 Recommendation also permits the Call Confirm packet to encode a different destination address when it encodes this facility. There are a number of reasons that can be encoded by the CLAMN facility. The Cisco X.25 hunt group implementation will cause the router to signal the hunt group event back to the X.25 Call originator using the CLAMN facility.

Caution X.25 security signaling facilities are used to explicitly notify the connecting stations of events that might raise security issues if they were not signaled. Suppression of these facilities should be configured only when the attached equipment and network configurations are sufficiently secure that the signaled information is unnecessary.

If no X.25 security issues apply, a network administrator may configure an X.25-class service to suppress the signaling of the CLAMN facility in Call Confirm packets using the **no x25 security clamn** command on an interface or x25 profile. This configuration may be necessary if the attached device or eventual recipient of the Call Confirm will not participate in a connection when the CLAMN security facility is encoded.

The X.25 Recommendations specify that the CLAMN facility must be present in the X.25 Call Confirm packet if that packet encodes a destination address that is not the null address and that differs from the address encoded in the Call packet. Therefore, when the **no x25 security clamn** command is used to suppress the encoding of the CLAMN facility, it will also suppress the encoding of the destination address; that is, if the address block is encoded in the Call Confirm packet, the destination address will be encoded as the null address (zero digits).

This command can be configured with the International Telecommunication Union Telecommunication Standardization Sector (ITU-T.) 1980 X.25 recommendation mode with no error, although the 1980 mode does not define the CLAMN facility.

Examples

The following example shows how to suppress the CLAMN security signaling facility:

```
interface serial 0
  no ip address
  encapsulation x25
  no x25 security clamn
```

Related Commands

Command	Description
no x25 security crcdn	Disables the CRCDN security signaling facility in X.25 Call packets transmitted.

x25 security crcdn

To reenable the Call Redirection/Call Deflection Notification (CRCDN) security signaling facility when it has been disabled, use the **x25 security crcdn** command in interface configuration mode. To disable the CRCDN security signaling facility in X.25 Call packets, use the **no** form of this command.

x25 security crcdn

no x25 security crcdn

Syntax Description

This command has no arguments or keywords.

Defaults

The CRCDN security signaling facility is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The X.25-class services use the CRCDN security signaling facility in X.25 call packets to notify the destination of the Call that a security event occurred during call processing. The encoding of this facility specifies the reason for the signal and the destination address that originally occurred in the call. There are a number of reasons that can be encoded by the CRCDN facility. The Cisco X.25 hunt group implementation will cause the router to signal the hunt group event to the X.25 call destination using the CRCDN facility.

Caution X.25 security signaling facilities are used to explicitly notify the connecting stations of events that might raise security issues if they were not signaled. Suppression of these facilities should be configured only when the attached equipment and network configurations are sufficiently secure that the signaled information is unnecessary.

If no X.25 security issues apply, a network administrator may configure an X.25-class service to suppress the signaling of the CRCN facility in call packets using the **no x25 security crcdn** command on an interface or X.25 profile. This configuration may be necessary if the attached device or eventual recipient of the X.25 call will not participate in a connection when the CRCDN security facility is encoded.

This command can be configured with the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) 1980 X.25 recommendation mode with no error, although the 1980 mode will always suppress the CRCDN facility.

Examples

The following example shows how to suppress the CRCDN security signaling facility:

```
interface serial 0
  no ip address
  encapsulation x25
  no x25 security crcdn
```

Related Commands

Command	Description
no x25 subscribe cug-service	Disables the CLAMN security signaling facility in X.25 Call Confirm packets and suppresses any destination address.

x25 subscribe cug-service

To enable and control standard closed user group (CUG) service, use the **x25 subscribe cug-service** command in the appropriate interface, line, or X.25 profile configuration mode. To disable standard CUG service, use the **no** form of this command.

x25 subscribe cug-service [**incoming-access**] [**outgoing-access**] [**suppress preferential** | **suppress all**]

no x25 subscribe cug-service [**incoming-access** | **outgoing-access**] [**suppress preferential** | **suppress all**]

Syntax Description

incoming-access	(Optional) Allows incoming access from the open network to the data terminal equipment (DTE) device.
outgoing-access	(Optional) Allows outgoing access from the data terminal equipment (DTE) device to the open network.
suppress preferential	(Optional) Suppresses CUG selection facility for the preferred CUG. This option is not available when configuring terminal lines.
suppress all	(Optional) Suppresses CUG selection facility for all CUGs. This option is not available when configuring terminal lines.

Defaults

No incoming access and no outgoing access. (This is the most restrictive setting.)
CUG selection facilities are not suppressed.

Command Modes

Interface configuration
Line configuration
X.25 profile configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	The **suppress preferential** and **suppress all** keywords were added to enable CUG selection facility suppression.
12.2(13)T	This command was modified to configure support for X.25 CUG service on terminal lines.
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 entering this command, specify the **incoming-access** or the **outgoing-access** keyword or both, unless you intend to have neither incoming nor outgoing access on the interface.

This command assumes that an X.25 network connection is being implemented and observes rules defined by X.25 and X.301 for CUG access. This command is enabled on a per-interface or per-line basis. Use this command to modify existing specified options without otherwise affecting the CUGs already defined.

The **x25 subscribe cug-service** command can be used to configure CUG security on synchronous X.25 data communications equipment (DCE) interfaces or terminal lines. A CUG service can be applied to console lines, auxiliary lines, standard asynchronous lines, and virtual terminal lines. A line configured for CUG service will apply CUG security to packet assembler/disassembler (PAD), X.28 mode, and protocol translation sessions. CUG protection is applied to incoming calls destined for the terminal line and call requests specified from the line.

The CUG selection facility suppression options are not available for terminal lines because incoming PAD calls are terminated by the line.

Use the **x25 subscribe cug-service** command with the **suppress preferential** or **suppress all** keywords to configure CUG selection facility suppression. The CUG selection facility suppression options are available on synchronous X.25 DCE interfaces only; they are not available on terminal lines because incoming PAD calls are terminated by the line.

The following restrictions apply to the **x25 subscribe cug-service** command:

- Disabling this command deconfigures all the CUGs defined for the device and disables all CUG-related commands, but it does not terminate the associated CUG switched virtual circuit (SVC) connections.
- The DTE cannot call the open part of the network unless the **outgoing-access** option is configured. Even if **outgoing-access** is permitted, the DCE will enforce any additional CUG requirements when handling an outgoing call (call request) from the DTE.
- The DTE will not receive calls from the open part of the network unless the **incoming-access** option is configured. Even if **incoming-access** is permitted, the DCE will enforce any additional CUG requirements before presenting an incoming call to the DTE.

Examples

CUG Service on a Terminal Line: Example

The following example shows the configuration of CUG behavior on asynchronous line 1 and virtual terminal lines 0 to 9. The users of virtual terminal lines 0 to 9 have access only within the corporate CUGs designated for engineering (CUG 1102 or 1103); any call from a network X.25-class service destined for the line will be refused unless the inbound point of presence (POP) has validated it as a member of one of those two CUGs.

```
line vty 0 9
 Location Company A. Engineering Access
 x25 subscribe cug-service
 x25 subscribe local-cug 2 network-cug 1102 preferential
 x25 subscribe local-cug 3 network-cug 1103
```

CUG Service with CUG Selection Facility Suppression and Incoming Access: Example

In the following example, CUG selection facility suppression and incoming access are configured for all CUGs, including the preferred CUG on the X.25 profile:

```
x25 profile CUG-SUPRS-ALL dce
 x25 subscribe cug-service incoming-access suppress all
 x25 subscribe local-cug 0 network-cug 10 preferential
 x25 subscribe local-cug 20 network-cug 202
 x25 subscribe local-cug 40 network-cug 40
```

CUG Service with Incoming and Outgoing Access: Example

The following example shows subscribing to both incoming and outgoing CUG service on the interface:

```
interface serial0
 encapsulation x25 dce
 x25 subscribe cug-service incoming-access outgoing-access
```

Related Commands

Command	Description
show x25 cug	Displays information about all CUGs or specific CUGs.
x25 facility	Forces facilities on a per-call basis for calls originated by the router.
x25 map	Sets the maximum number of virtual circuits that a protocol can have open simultaneously to one host.
x25 subscribe local-cug	Configures subscription to a specific CUG.

x25 subscribe flow-control

To control flow control parameter negotiation facilities in call setup packets, use the **x25 subscribe flow-control** command in interface or X.25 profile configuration mode. To have flow control parameter negotiation facilities included in call setup (outgoing) packets only when their values differ from the default values, use the **no** form of this command.

x25 subscribe flow-control {**always** | **never**}

no x25 subscribe flow-control

Syntax Description

always	Flow control parameter negotiation facilities are enabled and the flow control parameters are always included with call setup packets and are optional on inbound packets.
never	Flow control parameter negotiation facilities are disabled and the flow control parameters are never included with call setup packets, and are not permitted on inbound packets. Negotiation of flow control parameters is disabled.

Defaults

Flow control parameter negotiation facilities are included only when the parameter values differ from the default values.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
12.0(7)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 has three states—default behavior (**no x25 subscribe flow-control**), facilities **always** included, or facilities **never** included (flow control parameter negotiation is not enabled).

This command controls inclusion of the X.25 flow control parameter negotiation facilities in call setup packets. By default, these facilities are included in call setup packets only when their values differ from the default values.

Configuring the **no x25 subscribe flow-control** command restores the default behavior. This only includes facilities outbound call setup packets when the requested values do not match the interface defaults.

This command can also be used in X.25 profile configuration mode.

Examples

The following example shows flow control parameter negotiation disabled on serial interface 1/4:

```
Router(config)# interface serial 1/4
Router(config-if)# x25 subscribe flow-control never
```

Related Commands

Command	Description
x25 profile	Configures an X.25 profile without allocating any hardware-specific information.
x25 routing	Enables X.25 switching or tunneling.
x25 subscribe packetsize	Sets permitted and target ranges for packet size during flow control negotiation.
x25 subscribe windowsize	Sets permitted and target ranges for window size during flow control negotiation.

x25 subscribe local-cug

To configure subscription to a specific closed user group (CUG), use the **x25 subscribe local-cug** command in interface configuration or line configuration mode. To remove the CUG subscription, use the **no** form of this command.

x25 subscribe local-cug *number* **network-cug** *number* [**no-incoming** | **no-outgoing** | **preferential**]

no x25 subscribe local-cug *number* **network-cug** *number* [**no-incoming** | **no-outgoing** | **preferential**]

Syntax Description

number	Specific local CUG number (0 to 9999).
network-cug	Network translated CUG identifier.
number	Specific network CUG number (0 to 9999).
no-incoming	(Optional) Bars calls to data terminal equipment (DTE) within the specified CUG, unless **x25 subscribe cug-service incoming-access** is configured.
no-outgoing	(Optional) Bars calls from DTE within the specified CUG, unless **x25 subscribe cug-service outgoing-access** is configured.
preferential	(Optional) Specified on only one CUG, which is the assumed CUG when none is provided in call setup. (A single CUG listed at the interface is automatically considered a preferred CUG.)

Defaults

Incoming and outgoing access.
Preferential (if this is the only CUG specified).

Command Modes

Interface configuration
Line configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(13)T	This command was modified to configure X.25 CUG subscription on terminal lines.
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 first **x25 subscribe local-cug** command in a group of configurations will automatically enable CUG service behavior on the interface or line, if it is not already enabled, with the default setting of no public access.

The **x25 subscribe cug-service** command can be used to configure CUG subscription on X.25 synchronous data communications equipment (DCE) interfaces, console lines, auxiliary lines, standard asynchronous lines, and virtual terminal lines. A line configured for CUG service will apply CUG security to packet assembler/disassembler (PAD), X.28 mode, and protocol translation sessions. CUG protection is applied to incoming calls destined for the terminal line and call requests specified from the line.

A CUG number has only local significance. Because CUG service is a cooperative process among the network attachments (DCE devices), the local CUG number may have to be translated into a number that is significant to the network as a whole. For instance, two DTE devices may use CUG numbers 1 and 5 to refer to the global CUG number 1043 of the network. In this instance, both DCE devices would be configured to translate between the local CUG number of their DTE and the network CUG number. Duplicate network CUG identifiers are permitted for different local CUG identifiers.

A DTE subscription to a CUG that also includes the **no-incoming** option prevents incoming calls on that CUG (however, the DTE may still receive calls within other CUGs to which it is subscribed, or from the open network if incoming public access is subscribed).

CUG subscription of a DTE will not permit an outgoing call (call request) from the CUG if the **no-outgoing** option is configured.

The CUG will be assumed to be set to **preferential** (preferred) if there is only one CUG subscribed on that interface.

Examples

X.25 CUG Subscription on an Interface: Example

The following example subscribes local CUGs 5000, 100, 200, and 300 to networks 55, 11, 22, and 33, respectively, with local CUG 5000 being set as the preferred CUG:

```
Router(config)# interface serial0
Router(config-if)# encapsulation x25 dce
Router(config-if)# x25 subscribe cug-service incoming-access outgoing-access
Router(config-if)# x25 subscribe local-cug 5000 network-cug 55 preferential
Router(config-if)# x25 subscribe local-cug 100 network-cug 11
Router(config-if)# x25 subscribe local-cug 200 network-cug 22
Router(config-if)# x25 subscribe local-cug 300 network-cug 33
```

X.25 CUG Subscription on a Terminal Line: Example

The following example shows the configuration of CUG behavior on asynchronous line 1 and virtual terminal lines 0 to 9. The users of virtual terminal lines 0 to 9 have access only within the corporate CUGs designated for engineering (CUG 1102 or 1103); any call from a network X.25-class service destined for the line will be refused unless the inbound POP has validated it as a member of one of those two CUGs.

```
Router(config)# line vty 0 9
Router(config-line)# Location Company A. Engineering Access
Router(config-line)# x25 subscribe cug-service
Router(config-line)# x25 subscribe local-cug 2 network-cug 1102 preferential
Router(config-line)# x25 subscribe local-cug 3 network-cug 1103
```

Related Commands

Command	Description
show x25 cug	Displays information about all or specific (defined by the local or network CUG number) CUGs.
x25 facility	Forces facilities on a per-call basis for calls originated by the router (switched calls are not affected).

Command	Description
x25 map	Sets the maximum number of virtual circuits a protocol can have open simultaneously to one host.
x25 subscribe cug-service	Enables and controls standard CUG behavior on an X.25 DCE interface.

x25 subscribe packetsize

To set permitted and target ranges for packet size during flow control negotiation, use the **x25 subscribe packetsize** command in interface configuration mode. To revert to the default packet size ranges, use the **no** form of this command.

x25 subscribe packetsize {[**permit** *wmin wmax*] [**target** *wmin wmax*]}

no x25 subscribe packetsize {[**permit** *wmin wmax*] [**target** *wmin wmax*]}

Syntax Description

permit	Permitted packet-size range identifier.
pmin	Minimum setting for packet size range (16 to 4096 by a power of two).
pmax	Maximum setting for packet size range (16 to 4096 by a power of two).
target	Target packet-size range identifier.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)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

The **x25 subscribe packetsize** command lets you specify the range of permitted and target values for packet size. These are called flow control parameter negotiation facilities. You can specify the permitted minimum and maximum packet sizes and target values for packet transmission (16 to 4096 as a power of two). Setting these values outside the permitted range will result in connection failure. The router attempts to negotiate values within the target range, but will only allow values outside the target range to be negotiated as long as the negotiation complies with the procedure defined in X.25 recommendations.

This command should be configured separately on both the data terminal equipment (DTE) and data circuit-terminating equipment (DCE), so that the permit range will be compatible and calls will be able to pass through the network. The target range is less critical. It only needs to be set on the Cisco router conducting the switching.

The effective ranges will be further constrained by other configuration options including the selection of normal (modulo 8) or extended (modulo 128) sequence numbers, the maximum packet size supported by the interface, and the **x25 subscribe flow-control** command.

Examples

The following example shows X.25 local acknowledgment being configured on serial interface 1/4, with packet size ranges being set at a permitted rate of 64 (minimum) and 1024 (maximum) and target rate of 128 (minimum) and 1024 (maximum):

```
Router(config)# x25 routing acknowledge local
Router(config)# interface serial 1/4
Router(config-if)# encapsulation x25 dte
Router(config-if)# x25 subscribe packetsize permit 64 1024 target 128 1024
```

Related Commands

Command	Description
x25 routing	Enables X.25 switching or tunneling.
x25 subscribe windowsize	Sets permitted and target ranges for window size during flow control negotiation.
x25 subscribe flow-control	Controls flow control parameter negotiation facilities in call setup packets.

x25 subscribe throughput

To enable a router to negotiate X.25 throughput for end devices, use the **x25 subscribe throughput** command in interface configuration mode. To disable this feature, use the **no** form of this command.

x25 subscribe throughput {**never** | **basic**}

no x25 subscribe throughput

Syntax Description

never	Use this keyword for devices connected to the router that never expect the throughput facility field to be in the incoming call setup packets.
basic	Use this keyword for devices connected to the router that always expect the throughput facility field to be present in the incoming call setup packets.

Command Default

No X.25 throughput negotiation is performed by the router for end devices.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)YN	This command was introduced.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

Examples

In this example, the end device never expects the throughput facility field to be present in incoming call setup packets:

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/0
Router(config-if)# x25 subscribe throughput never
Router(config-if)# exit
```

In this example, the end device always expects the throughput facility field to be present in incoming call setup packets:

```
Router> enable
Router# configure terminal
Router(config)# interface serial0/0
Router(config-if)# x25 subscribe throughput basic
Router(config-if)# exit
```

In this example, the active throughput negotiation capability on the just-illustrated interface (Serial 0/0) is disabled:

```
Router(config)# interface serial0/0
Router(config-if)# no x25 subscribe throughput
Router(config-if)# exit
```

Related Commands

Command	Description
x25 facility throughput	Specifies the input and output bit rate values that the router should insert into the call setup packets' throughput-facility field.
x25 subscribe flow-control	Configures inclusion of X.25 flow-control parameter negotiation facilities in call setup packets.

x25 subscribe windowsize

To set permitted and target ranges for window size during flow control negotiation, use the **x25 subscribe windowsize** command in interface configuration mode. To revert to the default window size ranges, use the **no** form of this command.

x25 subscribe windowsize {[**permit** *wmin wmax*] [**target** *wmin wmax*]}

no x25 subscribe windowsize {[**permit** *wmin wmax*] [**target** *wmin wmax*]}

Syntax Description

permit	Permitted window size range identifier.
wmin	Minimum setting for window size range (1 to 127).
wmax	Maximum setting for window size range (1 to 127).
target	Target window-size range identifier.

Defaults

This command has no default values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)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

The **x25 subscribe windowsize** command lets you specify the range of permitted and target values for window size. These are called flow control values. You can specify the permitted minimum and maximum window size permitted and target values for packet transmission (1 to 127) at one time. Setting these values outside the permitted range may result in connection failure. The router attempts to negotiate values within the target range, but will only allow values outside the target range to be negotiated as long as the negotiation complies with the procedure defined in X.25 recommendations.

The effective ranges will be further constrained by other configuration options including the selection of normal (modulo 8) or extended (modulo 128) sequence numbers, the maximum window size supported by the interface, and the **x25 subscribe flow-control** command.

Examples

The following example shows X.25 local acknowledgment being configured on serial interface 1/4, with window size ranges being set at a permitted rate of 1 (minimum) and 7 (maximum) and target rate of 2 (minimum) and 4 (maximum):

```
Router(config)# x25 routing acknowledge local
Router(config)# interface serial 1/4
Router(config-if)# encapsulation x25 dte
Router(config-if)# x25 subscribe windowsize permit 1 7 target 2 4
```

Related Commands

Command	Description
x25 routing	Enables X.25 switching or tunneling.
x25 subscribe flow-control	Controls flow control parameter negotiation facilities in call setup packets.
x25 subscribe packetsize	Sets permitted and target ranges for packet size during flow control negotiation.

x25 suppress-called-address

To omit the destination address in outgoing calls, use the **x25 suppress-called-address** command in interface configuration mode. To reset this command to the default state, use the **no** form of this command.

x25 suppress-called-address

no x25 suppress-called-address

Syntax Description

This command has no arguments or keywords.

Defaults

The called address is sent.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include packet assembler/disassembler (PAD) calls.
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 omits the called (destination) X.121 address in Call Request packets and is required for networks that expect only subaddresses in the Called Address field.

Examples

The following example suppresses or omits the called address in Call Request packets:

```
interface serial 0
 x25 suppress-called-address
```

x25 suppress-calling-address

To omit the source address in outgoing calls, use the **x25 suppress-calling-address** command in interface configuration mode. To reset this command to the default state, use the **no** form of this command.

x25 suppress-calling-address

no x25 suppress-calling-address

Syntax Description

This command has no arguments or keywords.

Defaults

The calling address is sent.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include packet assembler/disassembler (PAD) calls.
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 omits the calling (source) X.121 address in Call Request packets and is required for networks that expect only subaddresses in the Calling Address field.

Examples

The following example suppresses or omits the calling address in Call Request packets:

```
interface serial 0
 x25 suppress-calling-address
```

x25 t10

To set the value of the Restart Indication retransmission timer (T10) on data communications equipment (DCE) devices, use the **x25 t10** command in interface configuration mode.

x25 t10 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

60 seconds

Command Modes

Interface configuration
X.25 profile 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.

Examples

The following example sets the T10 timer to 30 seconds:

```
interface serial 0
 x25 t10 30
```

x25 t11

To set the value of the Incoming Call timer (T11) on data communications equipment (DCE) devices, use the **x25 t11** command in interface configuration mode.

x25 t11 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

180 seconds

Command Modes

Interface configuration
X.25 profile 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.

Examples

The following example sets the T11 timer to 90 seconds:

```
interface serial 0
 x25 t11 90
```

x25 t12

To set the value of the Reset Indication retransmission timer (T12) on data communications equipment (DCE) devices, use the **x25 t12** command in interface configuration mode.

x25 t12 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

60 seconds

Command Modes

Interface configuration
X.25 profile 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.

Examples

The following example sets the T12 timer to 30 seconds:

```
interface serial 0
 x25 t12 30
```

x25 t13

To set the value of the Clear Indication retransmission timer (T13) on data communications equipment (DCE) devices, use the **x25 t13** command in interface configuration mode.

x25 t13 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

60 seconds

Command Modes

Interface configuration
X.25 profile 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.

Examples

The following example sets the T13 timer to 30 seconds:

```
interface serial 0
 x25 t13 30
```

x25 t20

To set the value of the Restart Request retransmission timer (T20) on data terminal equipment (DTE) devices, use the **x25 t20** command in interface configuration mode.

x25 t20 *seconds*

Syntax Description

seconds	Time in seconds.

Defaults

180 seconds

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.

Examples

The following example sets the T20 timer to 90 seconds:

```
interface serial 0
 x25 t20 90
```

x25 t21

To set the value of the Call Request timer (T21) on data terminal equipment (DTE) devices, use the **x25 t21** command in interface configuration mode.

x25 t21 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

200 seconds

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.

Examples

The following example sets the T21 timer to 100 seconds:

```
interface serial 0
 x25 t21 100
```

x25 t22

To set the value of the Reset Request retransmission timer (T22) on data terminal equipment (DTE) devices, use the **x25 t22** command in interface configuration mode.

x25 t22 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

180 seconds

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.

Examples

The following example sets the T22 timer to 90 seconds:

```
interface serial 0
 x25 t22 90
```

x25 t23

To set the value of the Clear Request retransmission timer (T23) on data terminal equipment (DTE) devices, use the **x25 t23** command in interface configuration mode.

x25 t23 *seconds*

Syntax Description

seconds	Time, in seconds.

Defaults

180 seconds

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.

Examples

The following example sets the T23 timer to 90 seconds:

```
interface serial 0
 x25 t23 90
```

x25 threshold

To set the data packet acknowledgment threshold, use the **x25 threshold** command in interface configuration mode.

x25 threshold *delay-count*

Syntax Description

delay-count	Value between zero and the input window size. A value of 1 sends one Receiver Ready acknowledgment per packet.

Defaults

0 (which disables the acknowledgment threshold)

Command Modes

Interface configuration
X.25 profile configuration

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

This command instructs the router to send acknowledgment packets when it is not busy sending other packets, even if the number of input packets has not reached the input window size count.

The router sends an acknowledgment packet when the number of input packets reaches the count you specify, providing there are no other packets to send. For example, if you specify a count of 1, the router will send an acknowledgment per input packet if it is unable to “piggyback” the acknowledgment of an outgoing data packet. This command improves line responsiveness at the expense of bandwidth.

This command only applies to encapsulated traffic over X.25 (datagram transport), not to routed traffic.

Examples

The following example sends an explicit Receiver Ready acknowledgment when it has received 5 data packets that it has not acknowledged:

```
interface serial 1
 x25 threshold 5
```

Related Commands

Command	Description
x25 win	Changes the default incoming window size to match that of the network.
x25 wout	Changes the default outgoing window size to match that of the network.

x25 use-source-address

To override the X.121 addresses of outgoing calls forwarded over a specific interface, use the **x25 use-source-address** command in interface configuration mode. To prevent updating the source addresses of outgoing calls, use the **no** form of this command.

x25 use-source-address

no x25 use-source-address

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration
X.25 profile 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

Some X.25 calls, when forwarded by the X.25 switching support, need the calling (source) X.121 address updated to that of the outgoing interface. This update is necessary when you are forwarding calls from private data networks to public data networks (PDNs).

Examples

The following example shows how to prevent updating the source addresses of outgoing X.25 calls on serial interface 0 once calls have been forwarded:

```
interface serial 0
 no x25 use-source-address
```

x25 version

To specify the X.25 behavior set that is to be used for X.25-class services (X.25, Annex G, and CMNS) and X.25 profiles, use the **x25 version** command in interface configuration mode or X.25 profile configuration mode. To restore the default value (the 1984 X.25 behavior set), use the **no** form of this command.

x25 version {**1980** | **1984** | **1988** | **1993**}

no x25 version

Syntax Description

1980	Specifies the 1980 CCITT X.25 behavior set.
1984	Specifies the 1984 CCITT X.25 behavior set. This is the default value.
1988	Specifies the 1988 CCITT X.25 behavior set.
1993	Specifies the 1993 ITU-T X.25 behavior set.

Defaults

The behavior set defined by the CCITT 1984 X.25 recommendation is used.

Command Modes

Interface configuration
X.25 profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9).

Usage Guidelines

The **x25 version** command is typically used to access functionality that is available in other X.25 behavior sets and to prevent problems that arise when a network is attached to X.25 devices that use nonstandard or older behavior sets. Table 126 describes some common problems that can be solved by specifying a particular X.25 behavior set.

Table 126 Common Problems That Are Solved by the x25 version Command

Problem	Cause	Solution
Some X.25 hosts reject calls that include Internetwork Call Redirection and Deflection Notification (ICRD) or Called Line Address Modification Notification (CLAMN).	X.25 hosts may conform to the 1980 standard, which does not support these facilities, or the host may be nonstandard.	Specify the 1980 X.25 behavior set on the interface or X.25 profile.
An incoming call that includes Protection QoS facilities (an ITU-T–specified DTE facility) is cleared by the Cisco router.	The interface defaults to the 1984 X.25 behavior set, which does not define the Protection QoS facility.	Specify the 1988 or 1993 behavior sets to allow Protection QoS facilities to be encoded and passed through transparently by the router.

Table 126 Common Problems That Are Solved by the x25 version Command (continued)

Problem	Cause	Solution
Incoming calls requesting a throughput of 64,000 bits per second (bps) are rejected while other calls requesting a throughput of 48,000 bps are accepted.	The throughput facility in the 1984 recommendation defines a maximum value of 48,000 bps.	Specify the 1988 behavior set for services where you need throughput facility values up to 64,000 bps, and the 1993 behavior set for services where you need throughput facility values up to 2,048,000 bps.
After a packet assembler/disassembler (PAD) call is initiated over X.25 over TCP (XoT), the Call is cleared by the router when the Call Confirm packet includes a modified destination address.	The called X.25 address has been modified on the Call Confirm by the remote X.25 host without signaling the fact by also encoding a CLAMN facility—a potential security issue.	If the security risks are acceptable, specify the 1980 behavior set on an X.25 profile configured for the XoT connection.

Examples

The following example configures an interface to use the 1980 X.25 behavior set:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface serial 3/2
Router(config-if)# x25 version 1980
Router(config-if)# end
```

The following example enables CMNS on Ethernet interface 0/0 and configures the interface to use the 1988 X.25 behavior set:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Ethernet0/0
Router(config-if)# cmns enable
Router(config-if)# x25 version 1988
Router(config-if)# end
```

The following example configures an X.25 profile to use the 1993 X.25 behavior set:

```
Router(config)# x25 profile annexg dxe
Router(config-if)# x25 version 1993
Router(config-if)# end
```

x25 win

To change the default incoming window size to match that of the network, use the **x25 win** command in interface configuration mode.

x25 win *packets*

Syntax Description

packets	Packet count that can range from 1 to one less than the window modulus.

Defaults

2 packets

Command Modes

Interface configuration
X.25 profile 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

This command determines the default number of packets a virtual circuit can receive before sending an X.25 acknowledgment. To maintain high bandwidth utilization, assign this limit the largest number that the network allows.

Note Set **x25 win** and **x25 wout** to the same value unless your network supports asymmetric input and output window sizes.

Examples

The following example specifies that 5 packets may be received before an X.25 acknowledgment is sent:

```
interface serial 1
 x25 win 5
```

Related Commands

Command	Description
x25 modulo	Sets the window modulus.
x25 threshold	Sets the data packet acknowledgment threshold.
x25 wout	Changes the default outgoing window size to match that of the network.

x25 wout

To change the default outgoing window size to match that of the network, use the **x25 wout** command in interface configuration mode.

x25 wout *packets*

Syntax Description

packets	Packet count that can range from 1 to one less than the window modulus.

Defaults

2 packets

Command Modes

Interface configuration
X.25 profile 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

This command determines the default number of packets a virtual circuit can send before waiting for an X.25 acknowledgment. To maintain high bandwidth utilization, assign this limit the largest number that the network allows.

Note Set **x25 win** and **x25 wout** to the same value unless your network supports asymmetric input and output window sizes.

Examples

The following example specifies a default limit of 5 for the number of outstanding unacknowledged packets for virtual circuits:

```
interface serial 1
 x25 wout 5
```

Related Commands

Command	Description
x25 modulo	Sets the window modulus.
x25 threshold	Sets the data packet acknowledgment threshold.
x25 win	Changes the default incoming window size to match that of the network.

x29 access-list

To limit access to the access server from certain X.25 hosts, use the **x29 access-list** command in global configuration mode. To delete an entire access list, use the **no** form of this command.

x29 access-list *access-list-number* {**deny** | **permit**} *x121-address*

no x29 access-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. It can be a value between 1 and 199.
deny	Denies access and clears call requests immediately.
permit	Permits access to the protocol translator.
x121-address	If applied as an inbound access class, specifies the X.121 address that can or cannot have access (with or without regular expression pattern-matching characters). The X.121 address is the source address of the incoming packet. If applied as an outbound access class, then the address specifies a destination to where connections are allowed.

Defaults

No access lists are defined.

Command Modes

Global 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

The **service pad** global configuration command must be configured before the **x29 access-list** command can be used.

An access list can contain any number of access list items. The list items are processed in the order in which you entered them, with the first match causing the permit or deny condition. If an X.121 address does not match any of the regular expressions in the access list, access is denied.

Access lists take advantage of the message field defined by Recommendation X.29, which describes procedures for exchanging data between two PADs, or between a PAD and a DTE device.

The UNIX-style regular expression characters allow for pattern matching of characters and character strings in the address. Various pattern-matching constructions are available that allow many addresses to be matched by a single regular expressions. For more information, refer to the “Regular Expressions” appendix in the *Cisco IOS Terminal Services Configuration Guide.*

The access lists must be applied to a vty with the **access-class** command.

Examples

The following example permits connections to hosts with addresses beginning with the string 31370:

```
x29 access-list 2 permit ^31370
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
service pad	Enables all PAD commands and connections between PAD devices and access servers.

x29 profile

To create a packet assembler/disassembler (PAD) profile script for use by the **translate** command, use the **x29 profile** command in global configuration mode.

x29 profile {**default** | *name*} *parameter*:*value* [*parameter*:*value*]

Syntax Description

default	Specifies default profile script.
name	Name of the PAD profile script.
parameter:*value*	X.3 PAD parameter number and value separated by a colon. You can specify multiple parameter-value pairs on the same line.

Defaults

The default PAD profile script is used. The default for inbound connections is:

```
2:0 4:1 15:0 7:21
```

Command Modes

Global 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

The **service pad** global configuration command must be configured before the **x29 profile** command can be used.

When an X.25 connection is established, the access server acts as if an X.29 Set Parameter packet had been sent containing the parameters and values set by the **x29 profile** command and sets the access server accordingly.

For incoming PAD connections, the Protocol Translator uses a default PAD profile to set the remote X.3 PAD parameters unless a profile script is defined with the **translate** command.

Note If you set the X.29 profile to "default," the profile is applied to all incoming X.25 PAD calls, including the calls used for protocol translation.

Examples

The following profile script turns local edit mode on when the connection is made and establishes local echo and line termination upon receipt of a Return packet. The name *linemode* is used with the **translate** command to effect use of this script.

```
x29 profile linemode 2:1 3:2 15:1
```

To override the default PAD profile, create a PAD profile script named “default” by using the following command:

```
x29 profile default 2:1 4:1 15:0 4:0
```

Related Commands

Command	Description
service pad	Enables all PAD commands and connections between PAD devices and access servers.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection type.

x29 inviteclear-time

To configure the time taken by the router to wait before responding to the X.29 invite clear message, use the **x29 inviteclear-time** command in global configuration mode. To disable the configuration, use the **no** form of this command.

x29 inviteclear-time *seconds*

no x29 inviteclear-time *seconds*

Syntax Description

seconds	Time, in seconds. The range is from 5 to 2147483.

Command Default

The router waits 30 seconds before responding to X.29 invite clear messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the response time of 6 seconds for the router to wait before responding to the X.29 invite clear message:

```
Router# enable
Router(config)# x29 inviteclear-time 6
```

Related Commands

Command	Description
show x29 access-lists	Displays X.29 access lists.
x29 access-list	Limits access to the access server from certain X.29 hosts.

xconnect

To bind an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

xconnect *peer-ip-address vc-id* {**encapsulation** {**l2tpv3** [**manual**] | **mpls** [**manual**]} | **pw-class** *pw-class-name*} [**pw-class** *pw-class-name*] [**sequencing** {**transmit** | **receive** | **both**}]

no xconnect

Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]

no xconnect *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*]

Syntax Description

peer-ip-address	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
vc-id	The 32-bit identifier of the virtual circuit (VC) between the PE routers.
encapsulation	Specifies the tunneling method to encapsulate the data in the pseudowire: • **l2tpv3**—Specifies Layer 2 Tunneling Protocol, version 3 (L2TPv3), as the tunneling method. • **mpls**—Specifies Multiprotocol Label Switching (MPLS) as the tunneling method. • **manual**—(Optional) Specifies that no signaling is to be used in the attachment circuit. This keyword places the router in xconnect configuration mode for manual configuration of the attachment circuit. Use this keyword to manually configure an AToM or L2TPv3 static pseudowire.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.
sequencing	(Optional) Sets the sequencing method to be used for packets received or sent. This keyword is not supported with the AToM Static Pseudowire Provisioning feature.
transmit	Sequences data packets received from the attachment circuit.
receive	Sequences data packets sent into the attachment circuit.
both	Sequences data packets that are both sent and received from the attachment circuit.
pw-type	(Optional) Pseudowire type. You can specify one of the following types: • 4—Specifies Ethernet VLAN. • 5—Specifies Ethernet port.

Command Default

The attachment circuit is not bound to the pseudowire.

Command Modes

Connect configuration (config-conn)
Interface configuration (config-if)
ATM PVC l2transport configuration (cfg-if-atm-l2trans-pvc)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(28)S	Support was added for Multilink Frame Relay connections.
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	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was updated to add support for AToM static pseudowires, and so that the remote router ID need not be the Label Distribution Protocol (LDP) router ID of the peer.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.
12.2(33)SXI5	This command was updated to add PFC3B or PFC3BXL restrictions for **xconnect**.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

The use of the **xconnect** command and the interface configuration mode bridge-group commands is not supported on the same physical interface.

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

Note If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on that router.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router. The VC ID creates the binding between a pseudowire and an attachment circuit.

With the introduction of VPLS Autodiscovery in Cisco IOS Release 12.2(33)SRB, the remote router ID need not be the LDP router ID. The address you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Note The VPLS Autodiscovery feature is not supported with L2TPv3.

For L2TPv3, to manually configure the settings used in the attachment circuit, use the **manual** keyword in the **xconnect** command. This configuration is called a static session. The router is placed in xconnect configuration mode, and you can then configure the following options:

- Local and remote session identifiers (using the **l2tp id** command) for local and remote PE routers at each end of the session.

- Size of the cookie field used in the L2TPv3 headers of incoming (sent) packets from the remote PE peer router (using the **l2tp cookie local** command).
- Size of the cookie field used in the L2TPv3 headers of outgoing (received) L2TP data packets (using the **l2tp cookie remote** command).
- Interval used between sending hello keepalive messages (using the **l2tp hello** command).

For L2TPv3, if you do not enter the **encapsulation l2tpv3 manual** keywords in the **xconnect** command, the data encapsulation type for the L2TPv3 session is taken from the encapsulation type configured for the pseudowire class specified with the **pseudowire-class** *pw-class-name* command.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.

Software prior to Cisco IOS Release 12.2(33)SRB configured pseudowires dynamically using Label Distribution Protocol (LDP) or another directed control protocol to exchange the various parameters required for these connections. In environments that do not or cannot use directed control protocols, the **xconnect** command allows provisioning an AToM static pseudowire. Use the **manual** keyword in the **xconnect** command to place the router in xconnect configuration mode. MPLS pseudowire labels are configured using the **mpls label** and (optionally) **mpls control-word** commands in xconnect configuration mode.

The following restrictions apply only if EARL modes are either PFC3B or PFC3BXL and you are running Cisco IOS Release 12.2(33)SXI4 or later releases on your router:

- SPAN is not allowed on an inband port if any physical interface has **xconnect** configured.
- SPAN is not allowed on a physical interface that also has **xconnect** configured.
- If an inband port has SPAN configured, then configuring **xconnect** on any physical interface results in a warning message. You should not proceed with this configuration because it can create an infinite packet loop.
- If a physical port has SPAN configured and you add **xconnect** on that same interface, a warning message is displayed and we strongly recommend that you do not proceed with such a configuration.

Examples

The following example configures xconnect service for an Ethernet interface by binding the Ethernet circuit to the pseudowire named 123 with a remote peer 10.0.3.201. The configuration settings in the pseudowire class named vlan-xconnect are used.

```
Router(config)# interface Ethernet0/0.1
Router(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect
```

The following example enters xconnect configuration mode and manually configures L2TPv3 parameters for the attachment circuit:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn) l2tp id 222 111
Router(config-if-xconn) l2tp cookie local 4 54321
Router(config-if-xconn) l2tp cookie remote 4 12345
Router(config-if-xconn) l2tp hello l2tp-defaults
```

The following example enters xconnect configuration mode and manually configures an AToM static pseudowire. The example shows the configuration for only one side of the connection; the configurations on each side of the connection must be symmetrical.

```
Router# configure terminal
Router(config)# interface Ethernet1/0
```

```
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
Router(config-if)# exit
```

The following example shows how to bind an attachment circuit to a pseudowire and configure an AToM service on a Cisco uBR10012 router:

```
Router# configure terminal
Router(config)# cable l2vpn 0000.396e.6a68 customer1
Router(config-l2vpn)# service instance 2000 Ethernet
Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming packets received from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing packets sent from the local PE peer router.
l2tp hello	Specifies the use of a hello keepalive setting contained in a specified L2TP class configuration for a static L2TPv3 session.
l2tp id	Configures the identifiers used by the local and remote provider edge routers at each end of an L2TPv3 session.
l2tp-class	Configures a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes.
mpls control-word	Enables the MPLS control word in an AToM static pseudowire connection.
mpls label	Configures an AToM static pseudowire connection by defining local and remote pseudowire labels.
mpls label range	Configures the range of local labels available for use on packet interfaces.
pseudowire-class	Configures a template of pseudowire configuration settings used by the attachment circuits transported over a pseudowire.
show xconnect	Displays information about xconnect attachment circuits and pseudowires.

xconnect backup force-switchover

To manually force a switchover to an attachment circuit or a pseudowire peer, use the **xconnect backup force-switchover** command in privileged EXEC mode.

xconnect backup force-switchover interface {*interface-info* | **peer** *ip-address vcid*}

Syntax Description

interface *interface-info*	Specifies the interface to be used for the switchover.
peer *ip-address vcid*	Specifies the IP address and virtual circuit (VC) ID of the VC to be used for the switchover.

Command Default

The pseudowire VC will not be changed.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

You can perform a switchover only to an available member in the redundancy group. That is, if the member being specified in the **xconnect backup force-switchover** command is not available, the command will be rejected.

Examples

The following example shows a Multiprotocol Label Switching (MPLS) xconnect with two redundant peers. The primary xconnect is using IP address 10.55.55.1, VC ID 500.

```
Router(config)# interface fastethernet1/0
Router(config-if)# xconnect 10.55.55.1 500 encapsulation mpls
Router(config-if-xconn)# backup peer 10.55.55.2 501
!
Router# xconnect backup force-switchover peer 10.55.55.2 501
```

Entering the **xconnect backup force-switchover** command will cause the router to switch to the pseudowire with an IP address of 10.55.55.2, VC ID 501.

To switch back to the primary pseudowire, enter the following command:

```
Router# xconnect backup force-switchover peer 10.55.55.1 500
```

If the xconnect cannot be switched over to the redundant pseudowire specified by the user, the standard redundancy algorithm will run and select either the primary or the highest secondary VC, depending on current availability.

The following example shows a local switching connection with two redundant peers. The primary xconnect is VLAN subinterface FastEthernet0/1.1 using 802.1Q tag 10. The xconnect is currently established with one of the backup peers when the manual switchover is issued to the primary xconnect.

```
Router(config)# interface FastEthernet0/0
!
Router(config)# interface FastEthernet0/1.1
Router(config-if)# encapsulation dot1Q 10
!
Router(config)# connect eth-vln FastEthernet0/0 FastEthernet0/1.1 interworking ethernet
Router(config-if)# backup peer 10.55.55.2 501
!
Router# xconnect backup force-switchover interface FastEthernet0/1.1
```

Entering the **xconnect backup force-switchover** command will cause the router to switch back to the VLAN subinterface FastEthernet0/1.1. If the xconnect cannot be switched over to the primary VLAN subinterface specified by the user, the standard redundancy algorithm will run and select the highest secondary VC, depending on current availability.

Related Commands

Command	Description
backup delay	Specifies how long a backup pseudowire VC should wait before taking over after the primary pseudowire VC goes down.
backup peer	Configures a redundant peer for a pseudowire VC.

xconnect encapsulation mpls

To configure scalable EoMPLS [SEoMPLS] on a service instance, use the **xconnect encapsulation mpls** command in service instance mode. To delete the scalable EoMPLS [SEoMPLS] on a service instance, use the **no** form of this command.

xconnect *peer-id vc-id* **encapsulation mpls**

no xconnect *peer-id vc-id* **encapsulation mpls**

Syntax Description

peer-id	Specifies the peer's Label Distribution Protocol (LDP) router id.
vc-id	Assign a virtual connection identifier (VC ID) for the virtual connection between the two peer provider edge devices. The range is 1 to 4294967295.

Command Default

There are no point-to-point connections configured.

Command Modes

Service instance

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

On the ingress side, after proper encapsulation manipulations, packet is tunneled in a EoMPLS VC and transmitted on the core.

The xconnect under service instance is always Scalable EoMPLS. Under the main interface, the type is determined by the line card (hardware or Scalable EoMPLS). We recommend to keep the implementation as scalable EoMPLS for the main interface, to avoid differences in service. The main interface and the service instance xconnect can not coexist in the same physical interface.

Examples

The following example shows how to configure scalable EoMPLS on a service instance:

```
Router(config-if-srv)# xconnect 10.0.0.1 123 encapsulation mpls
```

Related Commands

Command	Description
show mpls l2 vc detail	Displays detail information related to the VC.

xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

xconnect logging redundancy

no xconnect logging redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Syslog reporting of the status of the xconnect redundancy group is disabled.

Command Modes

Global configuration (config)

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.

Usage Guidelines

Use this command to enable syslog reporting of the status of the xconnect redundancy group.

Examples

The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Router(config)# xconnect logging redundancy
```

Activating the primary member:

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

Activating the backup member:

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

xot access-group

To control access to X.25 over TCP (XOT) and allow IP addresses permitted by the access list to have unique X.25 configuration, use the **xot access-group** command in global configuration mode. To delete an XOT access group, use the **no** form of this command.

xot access-group *access-list-number* [**profile** *profile-name*]

no xot access-group *access-list-number*

Syntax Description

access-list-number	Number of a standard IP access list. The range is from 1 to 99.
profile *profile-name*	(Optional) X.25 profile to be associated with the access group.

Defaults

No XOT access group is defined, and default X.25 parameter settings apply to XOT connections.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **xot access-group** command allows you to create XOT access groups by associating an IP access list with XOT. The access list provides a pass or fail indicator of whether a particular IP address is authorized.

Only standard IP access lists are supported.

XOT access groups are sorted by access-group number. When a new XOT connection is made, the IP address is tested against the access list of the first access group. If the IP address does not match the first list, the second list is tested, and so on.

The **xot access-group** command disables the legacy XOT functionality and enables the new XOT access behavior. If you enter the **xot access-group** after the legacy XOT context has been created, the message "Active connection(s) will terminate [confirm]" will be displayed if any XOT connections are active. If the message is confirmed, any active XOT connections using the legacy context will be detached. The legacy context will then be deleted.

Deleting an XOT access group by entering the **no xot access-group** command will cause the message "Active connection(s) will terminate [confirm]" to be displayed if any connections are active. Confirming the message will cause active connections using the access list to be detached and the associated XOT context to be deleted.

XOT access groups can be associated with X.25 profiles. By this means, the IP addresses specified in the access list can have a unique X.25 configuration. An access group can be associated with one X.25 profile. If an access group is not associated with an X.25 profile, then the XOT connections associated with the access group will use the default X.25 configuration.

The X.25 profile must already exist and must specify a data exchange equipment (DXE) station type before it can be associated with an XOT access group. The station type of a profile cannot be changed once the profile is created.

An X.25 profile can be associated with multiple access groups.

Examples

Unrestricted XOT Access with Defined X.25 Parameters for All XOT Connections: Example

In the following example, an access list is defined to permit all XOT connections. All XOT connections will use the X.25 configuration defined in the X.25 profile called “NEW-DEFAULT”.

```
! Create a DXE station type profile with any name and configure the X.25 parameters under
! the named profile
!
x25 profile NEW-DEFAULT dxe
 x25 address 12345
 x25 modulo 128
 x25 win 15
 x25 wout 15
 x25 ips 256
 x25 ops 256
!
! Define an IP standard access list to permit any XOT connection
!
access-list 10 permit any
!
! Apply the access list and X.25 profile to all XOT connections
!
xot access-group 10 profile NEW-DEFAULT
```

Restricted XOT Access with Multiple X.25 Parameter Configurations: Example

In the following example, XOT connections permitted by access list 10 will use the default X.25 configuration. XOT connections permitted by access list 22 will use the X.25 configuration that is defined in the X.25 profile named TRANSPAC.

```
! Define the IP access lists by specifying an IP access list number and access condition
!
ip access-list standard 10
 permit 10.0.155.9
 deny any
ip access-list standard 22
 permit 171.69.0.0 0.0.255.255 log
 deny any
!
! Apply the default X.25 configuration to XOT connections permitted by access list 10
!
xot access-group 10
!
! Configure an X.25 profile with station type DXE
!
x25 profile TRANSPAC dxe
 x25 modulo 128
 x25 win 80
 x25 wout 80
 x25 default pad

! Apply the X.25 profile to XOT connections permitted by access list 22
!
xot access-group 22 profile TRANSPAC
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
show x25 context	Displays operating configuration status details of an X.25 link.
show x25 profile	Displays details of X.25 profiles on your router.
show x25 xot	Displays information for all XOT virtual circuits that match a given criterion.
x25 profile	Configures an X.25 profile without allocating any hardware-specific information.