sequence-interval through show platform software otv fp

sequence-interval

To assign sequential numbers to class-maps, use the **sequence-interval** command in 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	Specifies the sequential interval. The range is 1 to 65535.

Command Default

Class-maps are not assigned with sequential numbers.

Command Modes

Policy-map configuration (config-profile)

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 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 data-link connection identifier (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.

Release	Modification
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.

services host-service peering

To configure the Secure Sockets Layer (SSL)-Express accelerator host peering service, use the **services host-service peering** command in WAAS SSL configuration mode.

services host-service peering

Syntax Description

This command has no arguments or keywords.

Command Default

Host peering service is enabled.

Command Modes

WAAS SSL configuration (config-waas-ssl)

Command History

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

Usage Guidelines

SSL peering service configuration parameters control secure communications established by SSL-Express accelerator between WAAS Express devices while optimizing SSL connections.

Host peering service is enabled as soon as WAAS Express is enabled on a WAN interface. Host peering service is enabled with the default configurations for **peer-ssl-version**, **peer-cipherlist**, and **peer-cert-verify enable** commands. In the default state, the **services host-service peering** command does not display in the output of the **show running-config all** command. It displays in the **show running-config all** command output if any of the **peer-ssl-version**, **peer-cipherlist**, or **peer-cert-verify enable** command is modified.

To customize the **peer-ssl-version**, **peer-cipherlist**, or **peer-cert-verify enable** command, use the **services host-service peering** command in WAAS SSL configuration mode to enter SSL peering service configuration mode.

The **services host-service peering** command is used to enter SSL peering configuration mode. To exit SSL peering configuration mode, use the **exit** command in SSL peering configuration mode.

Examples

The following example shows how to customize a host peering service:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator ssl-express
Device(config-waas-ssl)# enable
Device(config-waas-ssl)# services host-service peering
Device(config-waas-ssl-peering)# peer-ssl-version ssl3
```

Related Commands

Command	Description
accelerator	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
parameter-map type waas	Configures WAAS Express global parameters.
peer-cert-verify enable	Enables the verification of the peer certificate.
peer-cipherlist	Creates a cipher list to be used for WAAS-to-WAAS sessions.
peer-ssl-version	Configures the SSL version to be used for WAAS-to-WAAS sessions.
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or VC class.
show waas accelerator	Displays information about WAAS Express accelerators.
show waas statistics accelerator	Displays statistical information about WAAS Express accelerators.
waas enable	Enables WAAS Express on a WAN interface.
waas-ssl-trustpoint	Associates a trustpoint with SSL-Express accelerator.

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**commandis 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.

Command Default

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**commandis 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.

Command	Description
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.

Command Default

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**commandis 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.

Command Default

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.

Command Default

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.

Command Default

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

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
```

The table below describes the significant fields shown in the display.

Table 1: 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 ccm group

To display information about cluster control manager (CCM) groups on high availability (HA) Route Processor Stateful Switchover (RP-SSO) or Interchassis Stateful Switchover (IC-SSO) systems, use the **show ccm group** command in privileged EXEC mode.

show ccm group {**all**| **id** *group-id*}

Syntax Description

all	Displays information about all CCM groups (default, active, and inactive) configured on the router.
id	Displays the CCM group by group ID.
group-id	Valid existing CCM group ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

Use the **show ccm group** command to display either all CCM redundancy groups with their group numbers or a specific CCM redundancy group, along with the number of CCM sessions in each group, the type of HA infrastructure, and the redundancy state of each group.

Examples

The following is sample output from the **show ccm group all** command:

```
Device# show ccm group all
CCM Default Group(RP-SSO) Details
---------------------------------
CCM Group ID              : 0
Infra Group ID            : Not Applicable
Infra Type                : Redundancy Facility (RF)
HA State                  : CCM HA Active
Redundancy State          : Collecting
Group Initialized/cleaned : Not Applicable
CCM Non-default Group(Inter-Box HA) Details
-------------------------------------------
 CCM Group 1 Details
-----------------------
CCM Group ID              : 1
Infra Group ID            : 1
Infra Type                : Redundancy Group Facility (RGF)
HA State                  : CCM HA Active
Redundancy State          : Dynamic Sync
```

The following is sample output from the **show ccm group id** command:

```
Device# show ccm group id 1
CCM Group 1 Details
---------------------------------------
CCM Group ID              : 1
Infra Group ID            : 1
Infra Type                : Redundancy Group Facility (RGF)
HA State                  : CCM HA Active
Redundancy State          : Dynamic Sync
Group Initialized/cleaned : FASLE
```

The table below describes the significant fields shown in the display. Any data not described in the table is either self-explanatory or used for Cisco internal debugging.

Table 2: show ccm group Field Descriptions

Field	Description
CCM Group ID	Group ID of the CCM group. The default group ID is 0.
Infra Group ID	The corresponding redundancy infrastructure ID for this CCM group. This ID also matches the corresponding APS group ID.
Infra Type	The HA infrastructure type (Redundancy Facility [RF] or RGF)
HA State	The current HA state of the CCM group (active, standby, or HA absent)
Redundancy State	The current redundancy state of sessions that belong to the CCM group.

Related Commands

Command	Description
show ccm sessions	Displays CCM session information about HA RP-SSO and IC-SSO systems.

show ccm sessions

To display information about cluster control manager (CCM) sessions on Route Processor Stateful Switchover (RP-SSO) or Interchassis Stateful Switchover (IC-SSO) systems, use the **show ccm sessions** command in privileged EXEC mode.

show ccm sessions [**id** *group-id*]

Syntax Description

id	Displays the CCM session by group ID.
group-id	Valid existing CCM group ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.1(3)S	This command was modified. The **id** *group-id* keyword-argument pair was added.

Usage Guidelines

Use the **show ccm sessions** command to display information about CCM sessions on active and standby processors, and also to display information about subscriber redundancy sessions configured using the **subscriber redundancy** command.

Examples

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router active processor:

```
Device# show ccm sessions
Global CCM state:                              CCM HA Active - Dynamic Sync
Global ISSU state:                             Compatible, Clients Cap 0x0
 Number of sessions in state Down:              0
 Number of sessions in state Not Ready:         0
 Number of sessions in state Ready:             0
 Number of sessions in state Dyn Sync:          0
Timeout: Timer Type   Delay    Remaining Starts    CPU Limit CPU Last
  ------------ -------- --------- --------- --------- --------
  Rate         00:00:01  -         2         -         -
  Dynamic CPU  00:00:10  -         0         90        0
```

The following is sample output from the **show ccm sessions** command on a Cisco 10000 series router standby processor:

```
Device# show ccm sessions
Global CCM state:                      CCM HA Standby - Collecting
```

```
Global ISSU state:                      Compatible, Clients Cap 0xFFE
                                        Current     Bulk Sent   Bulk Rcvd
                                        ----------- ----------- -----------
Number of sessions in state Down:       0           0           0
Number of sessions in state Not Ready:  0           0           0
Number of sessions in state Ready:      0           0           0
Number of sessions in state Dyn Sync:   0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router active processor:

```
Device# show ccm sessions
Global CCM state:                               CCM HA Active - Dynamic Sync
Global ISSU state:                              Compatible, Clients Cap 0xFFFE
          Current     Bulk Sent   Bulk Rcvd
                                        ----------- ----------- -----------
Number of sessions in state Down:       0           0           0
Number of sessions in state Not Ready:  7424        0           0
Number of sessions in state Ready:      0           0           0
Number of sessions in state Dyn Sync:   20002       28001       0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
Rate         00:00:01 -          924         -         -
         Dynamic CPU  00:00:10 -         0           90        2
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:20 -         18          -         -
```

The following is sample output from the **show ccm sessions** command on a Cisco 7600 series router standby processor:

```
Device# show ccm sessions
Global CCM state:                       CCM HA Standby - Collecting
Global ISSU state:                      Compatible, Clients Cap 0xFFE
                                        Current     Bulk Sent   Bulk Rcvd
                                        ----------- ----------- -----------
Number of sessions in state Down:       0           0           0
Number of sessions in state Not Ready:  8038        0           0
Number of sessions in state Ready:      20002       0           28001
Number of sessions in state Dyn Sync:   0           0           0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
Rate         00:00:01 -          0          -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         1           -         -
         RF Notif Ext 00:00:20 -         0           -         -
```

The following is sample output from the **show ccm sessions id** command on a Cisco 7600 series router:

```
Device# show ccm sessions
id
Global CCM state:                       CCM HA Active - Dynamic Sync
                                        Current     Bulk Sent   Bulk Rcvd
                                        ----------- ----------- -----------
Number of sessions in state Down:       0           0           31
Number of sessions in state Not Ready:  9           10          11
Number of sessions in state Ready:      0           0           56
Number of sessions in state Dyn Sync:   66          62          0
Timeout: Timer Type   Delay    Remaining Starts      CPU Limit CPU Last
         ------------ -------- --------- ----------- --------- --------
         Rate         00:00:01 -         0           -         -
         Dynamic CPU  00:00:10 -         0           90        0
         Bulk Time Li 00:08:00 -         0           -         -
         RF Notif Ext 00:00:01 -         0           -         -
         RGF Bulk Tim 00:05:00 -         1           -         -
```

The table below describes the significant fields shown in the display. Any data not described in the table is either self-explanatory or used for Cisco internal debugging.

Table 3: show ccm sessions Field Descriptions

Field	Description
Global CCM state	Displays the processor's active or standby status and its CCM state. For example: CCM HA Active - Dynamic Sync means that this is the active processor, standby is in STANDBY_HOT state, and CCM is ready to synchronize sessions. CCM HA Active - Collecting means that this is the active processor and there is no standby processor. CCM can collect sessions but cannot synchronize them to a standby processor. CCM HA Active - Bulk Sync means that this is the active processor and a standby processor is booting up. CCM is doing a bulk synchronization of sessions. CCM HA Standby- Collecting means that this is the standby processor and is in STANDBY_HOT state. CCM is collecting sessions for synchronizing if a switchover happens.
Global ISSU state	Compatible, Clients Cap 0xFFFE0 indicates that CCM is compatible for in-service software upgrade (ISSU) clients, that is, ISSU-compatible Cisco IOS versions are running on both processors. It also means that CCM has the client capability for clients in the bitmask 0xFFFE.
Current	CCM sessions currently ready for synchronization.
Bulk Sent	CCM sessions sent during bulk synchronization.
Bulk Rcvd	CCM sessions received during bulk synchronization.
Number of sessions in state Down	Sessions in the down state.
Number of sessions in state Not Ready	Sessions in the not ready state.
Number of sessions in state Ready	Sessions in the ready state.
Number of sessions in state Dyn Sync	Sessions in the dynamic synchronization state.

Field	Description
Timeout	Displays statistics for the following timers: Rate—Monitors the number of sessions to be synchronized per configured time period. Dynamic CPU—Monitors the CPU limit, number of sessions, delay, and allowed calls configured for dynamic synchronization parameters. Bulk Time Li—Monitors the time limit configured for bulk synchronization. RF Notif Ext—Monitors redundancy facility (RF) active and standby state progressions and events. Use the **subscriber redundancy** command to modify parameters that these timers monitor.
Delay	Timer delay (in hh:mm:ss) for bulk and dynamic synchronization of subscriber sessions.
Remaining	Indicates the remaining time in seconds before the timer expires.
Starts	Indicates the number of times the timer started.
CPU Limit	CPU usage percentage, a configurable value; default is 90 percent.
CPU Last	Indicates the last time the CPU limit timer was running.

Related Commands

Command	Description
show ccm clients	Displays CCM client information.
show ccm queues	Displays CCM queue information.
subscriber redundancy	Configures subscriber session redundancy policies.

show 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.

Command Default

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

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
```

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
```

The table below describes the fields seen in these displays.

Table 4: 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

To 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.

Release	Modification
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.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Examples

The following example shows the local interworking connections on a router:

```
Device# 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
```

The table below describes the significant fields shown in the display.

Table 5: show connection Field Descriptions

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.

Field	Description
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 **showethernetserviceevc**command in privileged EXEC mode.

show ethernet service evc[**detail**| **id** *evc-id* **[detail]**| **interface** *type number* **[detail]**]

Syntax Description

interface 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.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

Examples

Following is sample output from the **show ethernet service evc**command:

```
Device# 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
```

The table below describes the significant fields in the output.

Table 6: 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 service instances, use the **show ethernet service instance** command in privileged EXEC mode.

show ethernet service instance [**detail**| **id** *id* {**interface** *type number* [**detail**| **mac** {**security** [**address**| **last violation**| **statistics**]| **static address**}| **load-balance**| **mac-tunnel [detail]**]}| **platform**| **stats**| **interface** *type number* [**detail**| **load-balance**| **platform**| **stats**| **summary**]| **mac security** [**address**| **last violation**| **statistics**]| **platform**| **policy-map**| **stats**| **summary**]

Cisco ASR 901 Series Aggregation Services Router

show ethernet service instance [**detail**| **id** *id* **interface** *type number* [**detail**| **mac security** [**address**| **last violation**| **statistics**]| **platform**| **stats**]| **interface** *type number* [**detail**| **platform**| **stats**| **summary**]| **mac security** [**address**| **last violation**| **statistics**]| **platform**| **policy-map**| **stats**| **summary**]

Syntax Description

detail	(Optional) Displays detailed information about service instances, a specific service instance, or about a MAC tunnel service instance.
id	(Optional) Displays a specific service instance on an interface that does not map to a VLAN.
id	(Optional) Integer from 1 to 4294967295 that identifies a service instance on an interface that does not map to a VLAN.
interface	(Optional) Declares a specific interface selection for a specified service instance.
type	(Optional) Type of interface.
number	(Optional) Number of the interface.
mac	(Optional) Displays MAC address data.
security	(Optional) Displays the MAC security status of a specified service instance.
address	(Optional) Displays the secure addresses on the specified service instance.
last violation	(Optional) Displays the last violation recorded on the specified service instance.
statistics	(Optional) Displays MAC security statistics for the specified service instance.

static	(Optional) Displays MAC static address information.
address	(Optional) Displays MAC static addresses in a bridge domain.
load-balance	(Optional) Displays EtherChannel load-balancing information.
mac-tunnel	(Optional) Displays the MAC tunnel Ethernet service instance identifier.
platform	(Optional) Displays platform information for a specified service instance.
stats	(Optional) Displays statistics for a specified service instance.
summary	(Optional) Displays summary information about service instances.
policy-map	(Optional) Displays the policy map for service instances.
mac security	(Optional) Displays the MAC security status of the specified service instance for Cisco ASR 901 Series Aggregation Services Routers.

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.
12.2(33)SRD	This command was modified. The **address**, **detail**, **lastviolation**, **macsecurity**, **platform**, **statistics**, **stats**, and **summary** keywords were added.
12.2(33)SRE	This command was modified. The **address**, **mac-tunnel**, and **static** keywords were added.
15.0(1)S	This command was modified. The **load-balance** keyword was added.
15.1(2)S	This command was modified. The output was extended to include information about Layer 2 context service instances, service initiators associated with a Layer 2 context, and the control policy associated with a Layer 2 context service instance.

Release	Modification
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Router. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces). The output includes information about trunk ports, if applicable.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command is useful for system monitoring and troubleshooting.

Examples

The following is sample output from the **show ethernet service instance** command:

```
Device# show ethernet service instance

Identifier  Type      Interface             State     CE-Vlans
4           static    GigabitEthernet3/2    Down
```

The table that follows describes the significant fields shown in the display.

Table 7: show ethernet service instance Field Descriptions

Field	Description
Identifier	Service instance identifier.
Type	Service instance type, as applicable, such as Static, L2Context, Dynamic, or Trunk.
Interface	Interface type and number with which the service instance is associated.
State	Service instance operational status such as Up, Down, or AdminDown.
CE-Vlans	Customer edge (CE) device VLAN ID.

Following is sample output from the **show ethernet service instance detail** command. The output shows details of different service instances configured on a given platform.

```
Device# show ethernet service instance detail

Service Instance ID: 1
Service instance type: L2Context
Intiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
```

```
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0

Service Instance ID: 2
Service instance type: Dynamic

Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
```

Following is sample output from the **show ethernet service instance interface detail** command. The output shows details of service instances configured on a specific interface.

```
Device# show ethernet service instance interface ethernet 0/0 detail

Service Instance ID: 1
Service instance type: L2Context
Intiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0

Service Instance ID: 2
Service instance type: Dynamic

Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0

Service Instance ID: 3
Service instance type: static
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans: 10-20
Encapsulation: dot1q 201 vlan protocol type 0x8100

Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
```

Following is sample output from the **show ethernet service instance id interface detail** command. The output shows details of a specific service instance configured on an interface.

```
Device# show ethernet service instance id 1 interface ethernet 0/0 detail

Service Instance ID: 1
Service instance type: L2Context
Intiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
```

This is an example of output from the **show ethernet service instance detail** command on a Cisco ASR 901 Series Aggregation Services Router:

```
Device# show ethernet service instance id 1 interface gigabitEthernet 0/1 detail

Service Instance ID: 1
Associated Interface: GigabitEthernet0/13
Associated EVC: EVC_P2P_10
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 10 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
Pkts In Bytes In Pkts Out Bytes Out
214 15408 97150 6994800
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 10
```

This is an example of output from the **show ethernet service instance stats** command on a Cisco ASR 901 Series Aggregation Services Router:

```
Device# show ethernet service instance id 1 interface gigabitEthernet 0/13 stats

Service Instance 1, Interface GigabitEthernet0/13
Pkts In Bytes In Pkts Out Bytes Out
214 15408 97150 6994800
```

Table 8: show ethernet service instance Field Descriptions

Field	Description
Service Instance ID	Service instance identifier.
Service instance type	Type of service instance.
Initiators	Service initiators associated with the service instance.
Control Policy	Control policy associated with the service instance.
Associated Interface	Interface on which the service instance is configured.

Field	Description
Associated EVC	Ethernet virtual circuit (EVC) associated with a device.
L2protocol drop	Number of Layer 2 protocol data units (PDUs) dropped.
CE-Vlans	VLANs associated with a device.
Encapsulation	Type of encapsulation used to enable session-level traffic classification.
Interface	Interface type and number with which the service instance is associated.
State	Up or Down.
EFP Statistics	Traffic on the service instance.

Related Commands

Command	Description
clear ethernet service instance	Clears Ethernet service instance attributes such as MAC addresses and statistics and purges Ethernet service instance errors.
show ethernet service 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** command in 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 all 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.
Cisco IOS XE Release 3.5S	This command was integrated into Cisco IOS XE Release 3.5S to provide support for the Cisco ASR 903 Device. This command was modified to provide support for Ethernet Flow Points (EFPs) on trunk ports (interfaces). The output includes information about trunk ports, if applicable.
Cisco IOS XE Release 3.6S	This command was modified. The output was modified to display the number of the bridge domains associated with the EFPs on an interface, if applicable.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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

The following is an example of output from the **show ethernet service interface** command when the **detail** keyword is specified:

```
Device# 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
Bridge-Domains: 10,20,30
<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
```

The table below describes the significant fields in the output.

Table 9: 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.
Bridge-Domains	Bridge domains associated with the EFPs on the interface.
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
```

The table below describes the significant fields shown in the display.

Table 10: 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
```

The table below describes the significant fields shown in the above examples.

Table 11: 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.

Command	Description
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.

Command Default

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:

Examples

```
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
```

Examples

```
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
```

The table below describes the fields shown in the display.

Table 12: 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.

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.

Field	Description
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.
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 data-link connection identifier (DLCI) 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.
Cisco IOS XE Release	This command was integrated into Cisco IOS XE release.

Usage Guidelines

When no parameters are specified with this command, the output displays a summary of each 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 **show frame-relay fragment** command does not display any data in the in-frag and out-frag columns (displays 0) when high-priority data is flowing. The in-frag and out-frag columns are updated when low-priority data (only when packet size is greater than or equal to fragment size) is sent across the link.

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
```

The following table describes the fields shown in the display:

Table 13: 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.

Field	Description
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.
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.

Field	Description
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
```

The table below describes the significant fields shown in the display.

Table 14: show frame-relay iphc Field Descriptions

Field	Description
DLCI	The DLCI number that identifies the PVC.
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
```

The table below describes the fields shown in the display.

Table 15: 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.

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
```

The table below describes significant fields in this output.

Table 16: show frame-relay lapf Field Descriptions

Field	Description
Interface	Identifies the interface and indicates the line status (up, down, administratively down).

Field	Description
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.
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.

Field	Description
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 lm**i 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.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

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
```

The table below describes significant fields shown in the output.

Table 17: 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.

Field	Description
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.

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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.

Examples

This section contains the following examples:

Examples

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
```

Examples

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 ip address 10.0.0.2 255.255.255.0
 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 10.0.0.1 255.255.255.0
 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
```

Examples

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
```

The table below describes the significant fields shown in the displays.

Table 18: 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.
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.

Release	Modification
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

Examples

The following is sample output from the **show frame-relay multilink** command (see the table below 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 the table below 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
```

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 (see the table below 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
```

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 the table below 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 the table below 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
```

The table below describes significant fields shown in the displays.

Table 19: show frame-relay multilink Field Descriptions

Field	Description
Bundle	Bundle interface.
State	Operational state of the bundle interface.

Field	Description
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.

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.

Field	Description
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.
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.

Release	Modification
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.
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.

Release	Modification
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

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:

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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
```

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)
```

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
```

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.

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
```

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
```

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
```

The table below describes the significant fields shown in the displays.

Table 20: 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.

Field	Description
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.
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.

Field	Description
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.

Field	Description
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.
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.

Field	Description
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.

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.

Field	Description
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 .
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)
```

The table below describes the significant fields in the output display.

Table 21: 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
```

The table below describes significant fields shown in the output.

Table 22: 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.

Field	Description
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
```

The table below describes significant fields in the output.

Table 23: 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.

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

Examples

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#
```

Examples

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#
```

Examples

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#
```

Examples

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#
```

The table below describes the significant fields shown in the **show frame-relay vc-bundle** displays.

Table 24: 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-sv
c
*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
```

The table below describes the significant fields shown in the displays.

Table 25: 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 l2fib

To display information about a Layer 2 Forwarding Information Base (L2FIB), use the **show l2fib** command in privileged EXEC mode.

show l2fib {**bridge-domain** {**summary** | *bridge-domain-ID* [**port** [**detail**]| **detail** | **table** {**multicast**| **unicast**}| **address** {**multicast** [*source-address*] *group-address*| **unicast** *mac-address*}| **otv** {**decap**| **encap** *address*}]}| **log** {**error**| **event**}| **output-list** [*output-list-ID*]}

Syntax Description

bridge-domain	Displays the L2FIB bridge domain information.
summary	Displays summary information about a bridge domain.
bridge-domain-ID	ID of a bridge domain. The range is from 1 to 4096.
port detail	(Optional) Displays detailed information about the ports that are configured on a bridge domain.
detail	(Optional) Displays detailed information about the specified bridge domain.
table	(Optional) Displays the content of the specified bridge domain table.
multicast	Specifies the multicast address. This keyword is available only when the **table** keyword or the **address** keyword is configured.
unicast	Specifies the unicast address. This keyword is available only when the **table** keyword or the **address** keyword is configured.
address	(Optional) Displays information about a bridge domain address.
source-address	IPv4 source address. This argument is available only when the **address multicast** keyword is configured.
group-address	IPv4 group address or IPv4 multicast group prefix. This argument is available only when the **address multicast** keyword is configured.
mac-address	MAC address. This argument is available only when the **address unicast** keyword is configured.
otv	(Optional) Displays information about Overlay Transport Virtualization (OTV) tunnel adjacency.
decap	Displays information about OTV tunnel decapsulation adjacency. This argument is available only when the **otv** keyword is configured.

encap *address*	Displays information about OTV tunnel encapsulation adjacency for the specified encapsulated IPv4 address. This argument is available only when the **otv** keyword is configured.
log	Displays L2FIB logs.
error	Displays L2FIB error logs in the circular buffer.
event	Displays L2FIB event logs in the circular buffer.
output-list *output-list-ID*	Displays information about the specified output list.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

A bridge domain table consists of a unicast MAC address, a broadcast address, and IPv4 multicast entries.

Examples

The following is sample output from the **show l2fib bridge-domain port** command:

```
Router# show l2fib bridge-domain 10 port

Bridge Domain: 10
  Replicator Port Count : 3
  Port Information :
    Serv Inst: Te0/1/0:10, Refcount: 4
    Serv Inst: Ov1:10, Refcount: 4
    OTV Encap: 239.1.1.1, Refcount 2
```

The following is sample output from the **show l2fib bridge-domain table** command:

```
Router# show l2fib bridge-domain 10 table unicast

Bridge Domain : 10
  Unicast Address table size : 3
  Unicast Address table information :
    Mac: 0000.4817.1e7e, Adjacency: OTV Encap: 209.165.201.2
    Mac: 0000.4818.8a82, Adjacency: Serv Inst: Te0/1/0:10
    Mac: ffff.ffff.ffff, Adjacency: Olist: 2035, Ports: 2
```

The following is sample output from the **show l2fib bridge-domain address** command:

```
Router# show l2fib bridge-domain 10 address unicast 1.1.2

Bridge Domain             : 10
Mac                       : 0001.0001.0002
Reference Count           : 1
Epoch                     : 0
Producer                  : BD-ENG
Flags                     : Age out
Adjacency: Service Instance:
  ID                      : Te0/0/0:1
  Reference Count         : 3
```

```
  Bridge Domain           : 10
  Interface if num        : 3
```

The table below describes the significant fields shown in the display.

Table 26: show otv l2fib Field Descriptions

Field	Description
Bridge Domain	The ID of the bridge domain.
Replicator Port Count	Number of bridge domain ports.
Serv Inst	The service instance identifier.
Refcount	Number of references that exist for this adjacency.
OTV Encap	OTV encapsulation address.
Unicast Address table size	Number of MAC addresses in the bridge domain MAC address table.
Unicast Address table information	Details of MAC addresses in the bridge domain MAC address table.
Mac	MAC addresses of hosts in the site.
Adjacency	Adjacency or next hop.
Reference Count	Number of references that exist for this adjacency.
Epoch	The epoch number.
Producer	Producer of the route or next hop.
Flags	Attribute of the route or next hop.
Interface if num	The internal identifier of the interface.

Related Commands

Command	Description
show otv mroute	Displays the OTV multicast route information from the RIB.
show otv route	Displays the OTV MAC routes from the RIB.

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
```

The table below describes the significant fields shown in the display.

Table 27: 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.

Field	Description
LocID	Local ID of the tunnel.
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
```

The table below describes the significant fields shown in the display.

Table 28: 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.

Field	Description
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.
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
```

The table below describes the significant fields shown in the display.

Table 29: 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.

Field	Description
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
```

The table below describes the significant fields shown in the display.

Table 30: 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 [ipv6]** [*filter*]| **sequence** [*filter*]| **state** [*filter*]]

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 on the router.
filter	(Optional) One of the filter parameters defined in the table below.
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.
ipv6	(Optional) Displays IPv6 packet and byte-count statistics.
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.
Cisco IOS XE Release 2.6	The **ipv6** keyword was added. The **show l2tun session** command with the **all** and **l2tp all** keywords was modified to display IPv6 counter information.

Usage Guidelines

Use the **show l2tun session**command to display information about current L2TP sessions on the router.

The table below defines the filter parameters available to refine the output of the **show l2tun session**command.

Table 31: 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.

Syntax	Description
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
```

The table below describes the significant fields shown in the displays.

Table 32: 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.
Circuit state is	State of the Layer 2 circuit.
Local circuit state is	State of the local circuit.

Field	Description
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.

Field	Description
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.
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.

Field	Description
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
```

The table below describes the significant fields shown in the displays.

Table 33: 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.
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 tunnels configured on the router.
filter	(Optional) One of the filter parameters defined in the table below.
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.
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** keyword was added.
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.

The table below defines the filter parameters available to refine the output of the **show l2tun tunnel**command.

Table 34: 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. The range is 1 to 65535.

Syntax	Description
local-name *local-name remote-name*	Filters the output to display information for only the tunnel associated with the specified names. • *local-name* --Local tunnel name. • *remote-name* --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* --Remote tunnel name. • *local-name* --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
```

The table below describes the significant fields shown in the displays.

Table 35: 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.

Field	Description
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.

Field	Description
Unsent queuesize, max	Current size of the unsent queue and maximum size of the unsent queue since tunnel establishment.
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   172.16.0.0      0     172.16.0.1       0
30866 IP   115   172.16.0.0      0     172.16.0.1       0
```
35217 IP 115 172.16.0.0 0 172.16.0.1 0

The table below describes the significant fields shown in the display.

Table 36: show l2tun tunnel transport Field Descriptions

Field	Description
Total tunnels	Total number of tunnels established.

Field	Description
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
```

The table below describes the significant fields shown in the display.

Table 37: 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 tun nel 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
```

The table below describes the significant fields shown in the display.

Table 38: 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.

Field	Description
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.
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 39: 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
```

The table below describes the significant fields shown in the display.

Table 40: 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
```

The table below describes the significant fields shown in the display.

Table 41: 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.
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.

Field	Description
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 mdns cache

To display information about the resource records in the multicast Domain Name System (mDNS) cache, use the **show mdns cache** command in privileged EXEC mode.

show mdns cache [*name* | *type*]

Syntax Description

name	(Optional) Name of the resource record.
type	(Optional) Type of the mDNS cache resource record.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Use the **show mdns cache** command to display resource record data for all mDNS service discovery devices. This command lets you retrieve and resolve mDNS service discovery resource record information that is cached. The resource records belong to the Internet class are denoted by IN.

This command displays information about the following types of resource records:

- Services Resolved (SRV) Records: Records where the instance name to hostname resolution is complete.
- Point to Record (PTR) Records: Records listing all instances of the resource.
- A Records: Records where the IPv4 address resolution is complete.
- AAAA Records: Records where the IPv6 address resolution is complete.

This command also provides information about the Time to Live (TTL) value for each resource record. The TTL value denotes the time line for which the resource record can remain active in the cache.

The RR Record Data column displays miscellaneous information and notes about the resource records.

Examples

The following is a sample output from the **show mdns cache** command. The fields in the output are self-explanatory.

```
Device# show mdns cache

                                                    MDNS CACHE
============================================================================================
[<NAME>]                                  [<TYPE>] [<CLASS>] [<TTL>] [<RR Record Data>]
```

```
test._kwaas._tcp.local                  SRV     IN      117     0       0       5676
 nostg-win7-1.local

nostg-win7-1.local                      A       IN      117     1.1.1.6

_kwaas._tcp.local                       PTR     IN      4485    test._kwaas._tcp.local
```

Related Commands

Command	Description
debug mdns	Enables debugging of mDNS service discovery information.
show mdns requests	Displays information about the browse requests, pending service requests, and pending host resolve requests recorded during the mDNS service discovery process.
show mdns statistics	Displays information about the number of packets sent, received, and dropped in the device recorded during the mDNS service discovery process.

show mdns requests

To display information about the browse requests, pending service requests, and pending host resolve requests recorded during the multicast Domain Name System (mDNS) service discovery process, use the **show mdns requests** command in privileged EXEC mode.

show mdns requests [*name* | *type*]

Syntax Description

name	(Optional) Name of the mDNS request.
type	(Optional) Type of the mDNS service discovery request.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Usage Guidelines

Use the **show mdns requests** command to display information about the different mDNS service discovery requests. The different requests for which you can query, and later retrieve information about from the queue, are as follows:

- Browse Requests: Requests that are made for browsing through the other available devices to discover services of interest.
- Service Requests: Requests made to other Cisco IOS devices that have been identified to contain services of interest.
- Host Resolve Requests: Requests made to resolve the hostname to IPv4 and IPv6 addresses.

Examples

The following is sample output from the **show mdns requests** command. The fields in the output are self-explanatory.

```
Device# show mdns requests


MDNS Outstanding Requests
=========================================================
Request name  :   _kwaas._tcp.local
Request type  :   PTR
Request class :   IN
```

Related Commands

Command	Description
debug mdns	Enables debugging of mDNS service discovery information.
show mdns cache	Displays information about the resource records in the mDNS cache during the mDNS service discovery process.
show mdns statistics	Displays information about the number of packets sent, received, and dropped in the device during the mDNS service discovery process.

show mdns statistics

To display information about the number of packets sent, received, and dropped in the device during the multicast Domain Name System (mDNS) service discovery process, use the **show mdns statistics** command in privileged EXEC mode.

show mdns statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)S	This command was introduced.

Examples

The following is a sample output from the **show mdns statistics** command. The fields in the output are self-explanatory.

```
Device# show mdns cache


mDNS Statistics
mDNS packets sent     : 393
mDNS packets received : 1054
mDNS packets dropped  : 320
```

Related Commands

Command	Description
debug mdns	Enables debugging of mDNS service discovery information.
show mdns cache	Displays information about the resource records in the mDNS cache during the mDNS service discovery process.
show mdns requests	Displays information about the browse requests, pending service requests, and pending host resolve requests during the mDNS service discovery process.

show mlrib common log

To display the common Multilayer Routing Information Base (MLRIB) log buffers, use the **show mlrib common log** command in privileged EXEC mode.

show mlrib common log {**event**| **error**} [**all**| **unique**| **wrap**]

Syntax Description

event	Displays common event logs.
error	Displays common error logs.
all	Displays all the buffers.
unique	Displays unique entries in the buffer.
wrap	Displays wrapped entries in the buffer.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show mlrib common log** command:

```
Router# show mlrib common log event all

[10/04/11 14:53:41.526 2 279] MLRIB_COMMON_REGISTRATION: client state set: L2FIB moving to
 REGISTERED state
[10/04/11 14:53:45.638 4 3] MLRIB_COMMON_REGISTRATION: client state set: ISISL2 OTV Overlay1
 moving to REGISTERED state
[10/04/11 14:53:45.669 6 268] MLRIB_COMMON_REGISTRATION: client state set: IGMP Snoop moving
 to REGISTERED state
[10/04/11 14:53:47.063 7 245] MLRIB_COMMON_REGISTRATION: client state set: OTV APP UCAST
PRODUCER moving to REGISTERED state
```

The table below describes the significant fields shown in the display.

Table 42: show mlrib common log Field Descriptions

Field	Description
MLRIB_COMMON_REGISTRATION	
client state set	

Related Commands

Command	Description
show otv mroute	Displays the OTV multicast route information from the RIB.
show otv route	Displays the OTV MAC routes from the RIB.

show mlrib layer2 log

To display the Layer 2-specific Multilayer Routing Information Base (MLRIB) log buffers, use the **show mlrib layer2 log** command in privileged EXEC mode.

show mlrib layer2 log {**event**| **error**| **trace**} [**all**| **unique**| **wrap**]

Syntax Description

event	Displays Layer 2 event logs.
error	Displays Layer 2 error logs.
trace	Displays Layer 2 trace logs.
all	Displays all the buffers.
unique	Displays unique entries in the buffer.
wrap	Displays wrapped entries in the buffer.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show mlrib layer2 log** command:

```
Router# show mlrib layer2 log event all

[10/17/11 10:44:38.889 E5D 167] MLRIB_L2_REDISTRIBUTE: hndl mcast redist refresh msg: Rcvd
 msg length 20, redist id = 0x0 walk id 0x0client = ISISL2 OTV Overlay1
[10/17/11 10:44:38.889 E5E 167] MLRIB_L2_REDISTRIBUTE: hndl mcast redist refresh msg: found
 filter for redist id = 0x0
[10/17/11 10:44:38.889 E5F 167] MLRIB_L2_REDISTRIBUTE: redist walk setup: for vpn 0x1 and
client ISISL2 OTV Overlay1
[10/17/11 10:44:38.889 E60 167] MLRIB_L2_REDISTRIBUTE: snd redist walk resp msg: switch to
 hp msg ISISL2 OTV Overlay1 s=2 f=0x48 q=FALSE ri=0x0, wi=0x0
[10/17/11 10:44:38.960 E61 167] MLRIB_L2_REDISTRIBUTE: hndl mcast redist refresh msg: Rcvd
 msg length 28, redist id = 0x1 walk id 0x1client = OTV APP MCAST PRODUCER
```

The table below describes the significant fields shown in the display.

Table 43: show mlrib common log Field Descriptions

Field	Description
MLRIB_L2_REDISTRIBUTE	

Field	Description
hndl mcast redist refresh msg	
Rcvd msg length	
redist id	
redist walk setup	
snd redist walk resp msg	

Related Commands

Command	Description
show otv mroute	Displays the OTV multicast route information from the RIB.
show otv route	Displays the OTV MAC routes from the RIB.

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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.

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 otv

To display the Overlay Transport Virtualization (OTV) status and parameters, use the **show otv** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **[detail]**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
detail	(Optional) Displays detailed information about the overlay interface.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If an overlay interface is specified, information about only that overlay is displayed; otherwise, information about all overlays is displayed.

In a unicast-core network, the **otv control-group** and **otv data-group** commands are not configured. Therefore, fields displaying information about the control group and data group are not included in the output of the **show otv** in a unicast-core network.

Examples

The following example shows how to display OTV information about a multicast-core network:

```
Device# show otv overlay 1

Overlay Interface Overlay1
 VPN name                 : None
 VPN ID                   : 1
 State                    : UP
 AED Capable              : Yes
 IPv4 control group       : 224.0.0.1
 Mcast data group range(s): 239.0.0.1/8
 Join interface(s)        : GigabitEthernet 0/0/0
 Join IPv4 address        : 209.165.201.1
 Tunnel interface(s)      : Tunnel0
 Encapsulation format     : GRE/IPv4
 Site Bridge-Domain       : 100
 Capability               : Multicast-reachable
 Is Adjacency Server      : No
 Adj Server Configured    : No
 Prim/Sec Adj Svr(s)      : None
```

The following is sample output from the **show otv** command in a unicast-core network when an OTV edge device is configured as a primary adjacency server:

```
Device# show otv overlay 3

Overlay Interface Overlay3
 VPN name                 : otv_3
 VPN ID                   : 1
 State                    : UP
 AED Capable              : Yes
 Join interface(s)        : GigabitEthernet0/1/1
 Join IPv4 address        : 10.0.2.8
 Tunnel interface(s)      : Tunnel0
 Encapsulation format     : GRE/IPv4
 Site Bridge-Domain       : 2
 Capability               : Unicast-only
 Is Adjacency Server      : Yes
 Adj Server Configured    : No
 Prim/Sec Adj Svr(s)      : None
```

The following is sample output from the **show otv** command in a unicast-core network when an OTV edge device is configured as a secondary adjacency server:

```
Device# show otv overlay 3

Overlay Interface Overlay3
 VPN name                 : otv_3
 VPN ID                   : 1
 State                    : UP
 AED Capable              : Yes
 Join interface(s)        : GigabitEthernet0/3/3
 Join IPv4 address        : 172.16.1.8
 Tunnel interface(s)      : Tunnel0
 Encapsulation format     : GRE/IPv4
 Site Bridge-Domain       : 2
 Capability               : Unicast-only
 Is Adjacency Server      : Yes
 Adj Server Configured    : Yes
 Prim/Sec Adj Svr(s)      : 10.0.2.8
```

The following is sample output from the **show otv** command when an OTV edge device is configured to use primary and secondary adjacency servers:

```
Device# show otv overlay 3

Overlay Interface Overlay3
 VPN name                 : otv_3
 VPN ID                   : 1
 State                    : UP
 AED Capable              : Yes
 Join interface(s)        : GigabitEthernet0/1/1
 Join IPv4 address        : 192.168.1.5
 Tunnel interface(s)      : Tunnel1
 Encapsulation format     : GRE/IPv4
 Site Bridge-Domain       : 2
 Capability               : Unicast-only
 Is Adjacency Server      : No
 Adj Server Configured    : Yes
 Prim/Sec Adj Svr(s)      : 10.0.2.8/172.16.1.8
```

The table below describes the significant fields shown in the displays.

Table 44: show otv Field Descriptions

Field	Description
VPN name	The OTV VPN name configured on the overlay interface.
VPN ID	The ID allocated and used internally by Cisco IOS XE software.

Field	Description
State	The current state of the overlay interface.
AED Capable	Capability of the edge device to be authoritative for one or more VLANs. Valid values are Yes and No. Yes indicates that the edge device is capable of being authoritative for one or more VLANs. No indicates that the edge device is not capable of being authoritative, in which case, a reason is also displayed.
IPv4 control group	The IP multicast address used by OTV to form the overlay.
Mcast data group range(s)	IP multicast addresses used for sending local IP multicast packets across the core.
Join interface(s)	Interface used for sending Internet Group Management Protocol (IGMP) joins towards the core.
Join IPv4 address	The IPv4 address of the join interface, used as the source IP address of OTV packets sent towards the core.
Tunnel interface(s)	The tunnel interface automatically created by OTV to encapsulate and decapsulate OTV packets.
Encapsulation format	The format of OTV packets sent across the core.
Site Bridge-Domain	The ID of the bridge domain being used for internal site IS-IS peering.
Capability	The multicast or unicast capability of the core.
Is Adjacency Server	Status indicating whether the local edge device is configured to be an adjacency server.
Adj Server Configured	Status indicating whether this edge device is configured to use an adjacency server.
Prim/Sec Adj Svr(s)	IP addresses of the primary and secondary adjacency servers configured, if any.

Related Commands

Command	Description
interface overlay	Creates an OTV overlay interface.
otv adjacency-server unicast-only	Configures a local edge device as an adjacency server in a unicast-core network.
otv control-group	Configures the IP multicast group address for the control and broadcast traffic for the specified OTV network.

Command	Description
otv data-group	Configures one or more ranges of core provider multicast group prefixes for multicast data traffic for the specified OTV network.
otv use-adjacency-server unicast-only	Configures a local edge device to use a remote adjacency server in a unicast-core network.
show otv isis	Displays the IS-IS status and configuration.

show otv adjacency

To display Overlay Transport Virtualization (OTV) adjacency information, use the **show otv adjacency** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **adjacency**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If an overlay interface is specified, information about only that overlay is displayed; otherwise information for all overlays is displayed.

Examples

The following example shows how to display OTV adjacency information:

```
Router# show otv overlay 1 adjacency

Overlay 1 Adjacency Database
Hostname       System-ID      Dest Addr        Up Time   State
North          0026.cb0d.0800 209.165.201.13   0:37:10   UP
```

The table below describes the significant fields shown in the display.

Table 45: show otv adjacency Field Descriptions

Field	Description
Hostname	Dynamic hostname of the system.
System-ID	The MAC address of the remote system.
Dest Addr	The IP address of the remote edge device.
Up Time	Time since this adjacency has been up.
State	Adjacency state of the neighboring interface. Valid states are Down, Init, and Up.

Related Commands

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

show otv adjacency-server replication-list

To display the list of unicast destinations for which multicast traffic is replicated, use the **show otv adjacency-server replication-list** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **adjacency-server replication-list**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

If an overlay interface is specified, information about only that overlay is displayed; otherwise, information about all overlays is displayed.

Overlay Transport Virtualization (OTV) maintains the unicast IP address of each remote edge device in the overlay network in a unicast replication list (URL). One URL is maintained per overlay network. OTV marks each address in the URL as active or inactive depending on the unicast-only status of the local and remote edge devices.

Examples

The following is sample output from the **show otv adjacency-server replication-list** command to display the list of unicast destinations for which multicast traffic is replicated:

```
Device# show otv adjacency-server replication-list

Overlay 1 Unicast Replication List Database
Total num: 1

Dest Addr       Capability
10.10.10.2      Unicast
```

The table below describes the significant fields shown in the display.

Table 46: show otv adjacency-server replication-list Field Descriptions

Field	Description
Dest Addr	Specifies the IP address of the unicast destination.
Capability	Lists whether the destination is multicast- or unicast-capable.

Related Commands

Command	Description
otv adjacency-server unicast-only	Configures a local edge device as an adjacency server in a unicast-core network.
otv use-adjacency-server unicast-only	Configures a local edge device to use a remote adjacency server in a unicast-core network.

show otv arp-nd-cache

To display Layer 2 and Layer 3 addresses cached from Address Resolution Protocol (ARP) packet inspection, use the **show otv arp-nd-cache** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **arp-nd-cache**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If an overlay interface is specified, cache entries for only that overlay are displayed.

Examples

The following example shows how to display the Layer 2 and Layer 3 address mapping for remote MAC addresses:

```
Router# show otv arp-nd-cache

Overlay1 ARP/ND L3->L2 Address Mapping Cache
 BD       MAC             Layer-3 Address  Age (HH:MM:SS)
 2        0030.19d2.ec39  172.16.1.2       00:05:30
 2        0030.16d5.3a5d  172.16.1.15      00:04:19
 65       0030.17e8.a389  172.16.1.18      00:00:50
```

The table below describes the significant fields shown in the display.

Table 47: show otv arp-nd-cache Field Descriptions

Field	Description
BD	The ID of the bridge domain where the ARP cache entry was snooped.
MAC	The MAC address snooped from the ARP reply packet.
Layer-3 Address	The IP address snooped from the ARP reply packet.
Age (HH:MM:SS)	Time since the ARP cache was last refreshed.

Related Commands

Command	Description
otv suppress arp-nd	Suppresses sending the IPv4 ARP requests and IPv6 ND neighbor solicitations on an overlay network.
show otv isis	Displays the IS-IS status and configuration.

show otv data-group

To display Overlay Transport Virtualization (OTV) data group information, use the **show otv data-group** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **data-group** [**local**| **remote**] [**detail**] [**bridge-domain** *bridge-domain-ID*] [**delivery-source** *delivery-source-address*] [**delivery-group** *delivery-group-address*] [**instance** *OTV-instance-ID*] [**source** *source-address*] [**group** *group-address*] [**vlan** *vlan-ID*]

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
local	(Optional) Displays output only for local data group sources.
remote	(Optional) Displays output only for remote data group sources.
detail	(Optional) Displays detailed output.
bridge-domain *bridge-domain-ID*	(Optional) Filters output based on the specified bridge domain. The range is from 1 to 4096.
delivery-source *delivery-source-address*	(Optional) Filters output based on the specified IPv4 delivery source address.
delivery-group *delivery-group-address*	(Optional) Filters output based on the specified IPv4 delivery group address.
instance *OTV-instance-ID*	(Optional) Filters output based on the specified OTV instance. The range is from 0 to 127.
source *source-address*	(Optional) Filters output based on the specified IPv4 source address.
group *group-address*	(Optional) Filters output based on the specified IPv4 group address.
vlan *vlan-ID*	(Optional) Filters output based on the specified VLAN ID. The range is from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If an overlay interface is specified, mappings for only that overlay are displayed. If the **detail** keyword is specified, then the number of unmapped sources is displayed.

Examples

The following example shows how to display OTV data group information:

```
Router# show otv data-group

Flags:  D - Local active source dynamically detected
        S - Local active source statically configured
        J - Data group has been joined in the core
        U - Data group has not been joined in the core

Remote Active Sources for Overlay1
 BD    Active-Source   Active-Group    Delivery-Source  Delivery-Group  Flags
 2     10.0.2.1        232.0.0.1       209.165.201.10   232.5.0.1       U
 4     10.0.4.1        232.0.0.1       209.165.201.10   232.5.0.3       U
 5     10.0.5.1        232.0.0.1       209.165.201.10   232.5.0.4       J
Displayed 3 remote data-group mappings

Local Active Sources for Overlay1
 BD    Active-Source   Active-Group    Delivery-Source  Delivery-Group  Flags
 1     10.0.1.1        232.0.0.1       209.165.201.10   232.5.0.0       S
 2     10.0.2.1        232.0.0.1       209.165.201.10   232.5.0.1       D


Displayed 2 local data-group mappings
```

The table below describes the significant fields shown in the display.

Table 48: show otv data-group Field Descriptions

Field	Description
BD	The ID of the bridge domain where the multicast traffic was snooped.
Active-Source	The unicast IP source address of the multicast sender.
Active-Group	The multicast IP destination address used by the multicast sender.
Delivery-Source	The unicast IP source address used for forwarding the multicast traffic in the core.
Delivery-Group	The multicast IP destination address used for forwarding the multicast traffic in the core.

Related Commands

Command	Description
otv data-group	Configures one or more ranges of core provider multicast group prefixes for multicast data traffic for the specified OTV network.
show otv isis	Displays the IS-IS status and configuration.

show otv isis database

To display the contents of the Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) database for each overlay, use the **show otv isis database** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*] **database** [**mgroup**| **standard**] [**detail**| **verbose**] *lsp-ID*

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
mgroup	(Optional) Displays the IS-IS multicast database for each overlay.
standard	(Optional) Displays standard LSP information.
detail	(Optional) Displays detailed link state database IS-IS information.
verbose	(Optional) Displays verbose LSP information.
lsp-ID	LSP ID in the form of xxxx.xxxx.xxxx.xx-xx or *name*.xx-xx.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The output of this command can be used to determine the unicast MACs and multicast groups received from each neighbor.

Examples

The following is sample output from the **show otv isis database** command:

```
Router# show otv isis database detail

Tag Overlay1:
IS-IS Level-1 Link State Database:
LSPID      LSP Seq Num   LSP Checksum    LSP Holdtime   ATT/P/OL
u1.00-00   0x00000007    0x2B3A          1094           0/0/0
Area Address: 00
NLPID: 0xCC 0x8E
Hostname: u1
Layer 2 MAC Reachability: topoid 0, vlan 100, confidence 1
1122.3344.5566 2222.3344.5566
Layer 2 MAC Reachability: topoid 0, vlan 101, confidence 1
1122.7788.99aa 2222.7788.99aa
```

The table below describes the significant fields shown in the display.

Table 49: show otv isis database detail Field Descriptions

Field	Description
LSPID	LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. The last octet is the LSP number. If all data cannot fit into a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number.
LSP Seq Num	LSP sequence number that allows other systems to determine if they received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time (in seconds) for which the LSP remains valid. An LSP hold time of zero indicates that this LSP was purged and is being removed from all routers' link state databases (LSDBs). The value indicates how long the purged LSP will stay in the LSDB before it is completely removed.
ATT	Attach bit. This bit indicates that the router is also a Level 2 router and that it can reach other areas. Level 1 routers use the Attach bit to find the closest Level 2 router. They install a default route to the closest Level 2 router.
P	P bit. This bit detects if the IS can repair area partitions. Cisco and other vendors do not support area partition repair.
OL	Overload bit. This bit determines if the IS is congested. If the overload bit is set, other routers do not use this system as a transit router when they calculate routes. Only packets for destinations directly connected to the overloaded router are sent to this router.
Area Address	Reachable area addresses from the router. For Level-1 LSPs, these are the area addresses configured manually on the originating router. For Level-2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID	Network Layer Protocol (NLP) identifier.
Hostname	Hostname of the node.
Layer 2 MAC Reachability	Layer 2 MAC Reachability type, length, values (TLVs) and displays the MAC address that the IS is advertising, and the MAC address that can be reached from this IS.

Related Commands

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

show otv isis hostname

To display the Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) dynamic hostname table information, use the **show otv isis hostname** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*] **hostname**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis hostname** command:

```
Router# show otv isis hostname

Level System ID        Dynamic Hostname (Overlay1)
1     AABB.CC00.0100   u1
*     AABB.CC00.0300   u3
1     AABB.CC00.0200   u2
```

The dynamic hostname table in the example displays the router name-to-system ID mapping table entries for router u1, router u2, and the local router u3. The command output shows that the local router is running the IS-IS process named Overlay1. The table also shows that the neighbor routers u1 and u2 are Level-1 routers, and their hostnames are advertised by the Level-1 (L1) link-state packet (LSP). The * symbol that appears for the router u3 signifies that this is the router name-to-system ID mapping information for the local router.

The table below describes the significant fields shown in the display.

Table 50: show otv isis hostname detail Field Descriptions

Field	Description
Level	IS-IS level of the router. * indicates the local router.
System ID	The MAC address of the remote edge device.
Dynamic Hostname	The dynamic hostname of the edge device.

Related Commands

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

show otv isis lsp-log

To display the Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) logs, use the **show otv isis lsp-log** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*] **lsp-log**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

An entry in the LSP log is created each time a shortest path first (SPF) event is run along with a reason why SPF ran.

Examples

The following is sample output from the **show otv isis lsp-log** command:

```
Router# show otv isis lsp-log

Tag Overlay1:
Level 1 LSP log
When     Count Interface Triggers
00:47:11 3     Overlay1  CONFIG
00:46:58 2     Overlay1  NEWADJ DIS
00:45:44 1     Overlay1  CONFIG
00:44:58 1     Overlay1  CONFIG
00:21:51 4               CLEAR
00:20:49 4               CLEAR
00:20:46 4               CLEAR
00:19:01 2     Overlay1  DELADJ
00:18:45 2     Overlay1  NEWADJ DIS
00:18:06 4               CLEAR

Level 1 mgroup LSP log
When     Count Interface Triggers
00:47:11 2     Overlay1  CONFIG
00:45:44 1     Overlay1  CONFIG
00:44:58 1     Overlay1  CONFIG
00:18:45 2               CLEAR
```

The table below describes the significant fields shown in the display.

Table 51: show otv isis lsp-log detail Field Descriptions

Field	Description
When	Time elapsed (in hh:mm:ss) since the last LSP was generated.
Count	Number of events that took place at this time.
Interface	Interface that caused the LSP regeneration.
Triggers	Event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows: • AREASET—Active area set changed. • ATTACHFLAG—Attach bit changed state. • CLEAR—Some form of the manual **clear** command was issued. • CONFIG—Any configuration change. • DELADJ—Adjacency went down. • DIS—Designated Intermediate System (DIS) or pseudonode changed. • ES—End System adjacency changed. • HIPPITY—LSP Database (LSPDB) overload bit changed state. • IF_DOWN—Needs a new LSP. • IP_DEF_ORIG—Default information originate changed. • IPDOWN—Directly connected IP prefix down. • IP_EXTERNAL—Redistributed IP route appeared or gone. • IPIA—Interarea IP route appeared or gone. • IPUP—Directly connected IP prefix up. • NEWADJ—New adjacency came up. • REDIST—Redistributed level-2 Connectionless Network Service (CLNS) route changed. • RRR_INFO—RRR bandwidth resource information.

Related Commands

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

show otv isis neighbors

To display the adjacencies formed by Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) for each overlay, use the **show otv isis neighbors** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*| **site**] **neighbors** [**detail**]

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
site	(Optional) Configures the IS-IS Layer 2 site process.
detail	(Optional) Displays detailed information about adjacencies.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis neighbors** command:

```
Router# show otv isis neighbors

Tag Overlay1:
System Id   Type Interface  IP Address         State   Holdtime   Circuit Id
u1          L1   Ov1        209.165.201.22     UP      22         u3.01
```

The table below describes the significant fields shown in the display.

Table 52: show otv isis neighbors Field Descriptions

Field	Description
System Id	Six-byte value that identifies a system in an area.
Type	Level type. Indicates whether the IS-IS neighbor is a Level 1, Level-1-2, or Level 2 router.
Interface	Interface from which the system was learned.
IP Address	IP address of the neighbor router.
State	Indicates whether the state of the IS-IS neighbor is up or down.

Field	Description
Holdtime	Link-state packet (LSP) hold time. Amount of time (in seconds) for which the LSP remains valid.
Circuit Id	Port location for the IS-IS neighbor router that indicates how it is connected to the local router.

Related Commands

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

show otv isis nsf

To display the nonstop forwarding (NSF) state of Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS), use the **show otv isis nsf** command in privileged EXEC mode.

show otv isis nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis nsf** command:

```
Router# show otv isis nsf

Tag Overlay10:

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, RTR chkpt peer ready, UPD chkpt peer ready, bulk sync complete
 NSF interval timer expired (NSF restart enabled) Checkpointing enabled, no errors Local
state: ACTIVE,  Peer state: STANDBY HOT,  Config Mode: SSO, Operating Mode: SSO

Tag Site:

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, RTR chkpt peer ready, UPD chkpt peer ready, bulk sync complete
 Checkpointing enabled, no errors Local state: ACTIVE,  Peer state: STANDBY HOT,  Config
Mode: SSO, Operating Mode: SSO
```

The output is self-explanatory.

Related Commands

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

show otv isis protocol

To display information about the general state of the Overlay Transport Virtualization (OTV) Intermediate-System-to-Intermediate System (IS-IS) process and a summary of the default configuration parameters, overlays, and interfaces enabled, use the **show otv isis protocol** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*| **site**] **protocol**

Syntax Description

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

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis protocol** command:

```
Router# show otv isis protocol

Tag Overlay10:
IS-IS Router: Overlay10
  System Id: AABB.CC00.8100.00  IS-Type: level-1
  Manual area address(es):
        00
  Routing for area address(es):
        00
  Interfaces supported by IS-IS:
        Overlay10

Tag Site:
IS-IS Router: Site
  System Id: AABB.CC00.8100.00  IS-Type: level-1
  Manual area address(es):
        00
  Routing for area address(es):
        00
  Interfaces supported by IS-IS:
        OTV-Site
```

The table below describes the significant fields shown in the display.

Table 53: show otv isis protocol Field Descriptions

Field	Description
IS-IS Router	Identifier of an IS-IS instance on the router.
System Id	Identification value of the system.
Manual area address(es)	Area addresses that have been configured.
Routing for area address(es)	List of manually configured and learned area addresses.
Interfaces supported by IS-IS	List of interfaces on the router supporting IS-IS.

Related Commands

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

show otv isis rib

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

show otv isis rib [**overlay** *overlay-interface*] [**redistribution**] {**mac**| **multicast [mapping]**}

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
redistribution	(Optional) Displays IS-IS redistribution RIB information.
mac	Displays MAC addresses from the IS-IS RIB.
multicast	Displays multicast route information from the IS-IS RIB.
mapping	(Optional) Displays multicast mapping information from the IS-IS RIB.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis rib mac** command:

```
Router# show otv isis rib mac

Tag Overlay10:
 MAC  local rib for Overlay10 (Total 2)
  L2 Topology ID        Mac Address
  103                   1234.0002.0001
    [50/1] via 11.0.0.1(Overlay10), LSP[5/6]
  103                   1234.0002.0002
    [50/1] via 11.0.0.1(Overlay10), LSP[5/6]
```

The following is sample output from the **show otv isis rib multicast** command:

```
Router# show otv isis rib multicast

Tag Overlay10:
 MCAST  local rib for Overlay10 (Total Groups: 2, Sources: 4)
 L2 Topology ID    Source Address      Group Address
 103               192.0.1.1           224.0.0.1
    [50/1] via 192.0.2.1(Overlay10), LSP[6/6]
 103               192.0.2.1           224.0.0.1
    [50/1] via 192.0.2.1(Overlay10), LSP[6/6]
 103               192.0.1.1           224.0.0.2
    [50/1] via 192.0.2.1(Overlay10), LSP[6/6]
```

```
 103               192.0.2.1           224.0.0.2
    [50/1] via 192.0.2.1(Overlay10), LSP[6/6]
```

The following is sample output from the **show otv isis rib multicast mapping** command:

```
Router# show otv isis rib multicast mapping

Tag Overlay10:
 MCAST MAPPING   local rib for Overlay10 (Total Data/Delivery Groups: 4)
 Total Multicast Groups: 4, Sources: 4
 L2 Topology ID    Data Source     Data Group          Source          Group
 103               192.0.2.1       232.1.1.2           192.0.1.1       224.0.0.1
    [0/0] LSP[6/6]
 103               192.0.2.1       232.1.1.3           192.0.2.1       224.0.0.1
    [0/0] LSP[6/6]
 103               192.0.2.1       232.1.1.6           192.0.1.1       224.0.0.2
    [0/0] LSP[6/6]
 103               192.0.2.1       232.1.1.7           192.0.2.1       224.0.0.2
    [0/0] LSP[6/6]
```

The table below describes the significant fields shown in the display.

Table 54: show otv isis rib Field Descriptions

Field	Description
L2 Topology ID	Layer 2 topology ID.
Mac Address	Layer 2 route in the form of a unicast MAC Address.
[50/1]	Administrative instance/type/metric for the routing path to reach the next hop of the router.
via 192.0.2.1(Overlay10)	IP address of the next hop—in this instance, Overlay10.
Source Address	Unicast source IP (or IPv6) address for a multicast Layer 2 route entry.
Group Address	Multicast IP group address for a multicast Layer 2 route entry.
Data Source	Unicast source IP (or IPv6) address in the provider network for a multicast mapping entry.
Data Group	Multicast IP group address in the provider network for a multicast mapping entry.
Source	Unicast source IP (or IPv6) address on the access side of the overlay for a multicast mapping entry.
Group	Multicast IP group address on the access side of the overlay for a multicast mapping entry.

Related Commands

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

show otv isis spf-log

To display logs related to Overlay Transport Virtualization (OTV) Intermediate-System-to-Intermediate System (IS-IS) shortest path first (SPF) computation, use the **show otv isis spf-log** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*] **spf-log**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

An entry in the log is created each time SPF is run, along with a reason why it ran.

Examples

The following is sample output from the **show otv isis spf-log** command:

```
Router# show otv isis spf-log

Tag Overlay1:
TID 0 level 1 SPF log
When     Duration   Nodes    Count    First trigger LSP    Triggers
00:17:05 0          1        3        u3.00-00             PERIODIC LSPEXPIRED
00:16:54 0          1        3        u3.00-00             NEWADJ NEWLSP CHGTUNNEL
00:16:53 0          2        1        u3.01-00             LSPEXPIRED
00:16:48 0          2        2        u1.00-00             LSPEXPIRED
00:16:47 0          3        3        u1.00-00             LSPEXPIRED
00:10:38 0          3        1        0000.0000.0000.00-00 LSPHEADER
00:02:06 1          3        1                             PERIODIC
```

The table below describes the significant fields shown in the display.

Table 55: show otv isis spf-log Field Descriptions

Field	Description
When	The time elapsed (in hours: minutes: seconds) since the last full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Time (in milliseconds) required to complete this SPF run. Elapsed time is clock time, not CPU time.

Field	Description
Nodes	Number of routers and pseudonodes (LANs) that comprise the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits for 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting for 5 seconds before running full SPF.
First trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the first received LSP is remembered.
Triggers	A possible reason that triggered a full SPF calculation.

Related Commands

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

show otv isis vlan-database

To display information about Overlay Transport Virtualization (OTV) Intermediate System-to-Intermediate System (IS-IS) VLANs from the local database, use the **show otv isis vlan-database** command in privileged EXEC mode.

show otv isis [**overlay** *overlay-interface*] **vlan-database**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv isis vlan-database** command. The fields shown in the output are self-explanatory.

```
Router# show otv isis vlan-database

Tag Overlay1:
OTV IS-IS process: Overlay1
VPN name: Overlay1
Bridge Domain ID  OTV Instance ID  VLAN ID  AED Status
1100              0                100      ENABLED
1101              0                101      ENABLED
```

Related Commands

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

show otv log

To display the Overlay Transport Virtualization (OTV) debug log of events or errors, use the **show otv log** command in privileged EXEC mode.

show otv log {**event**| **error**}

Syntax Description

event	Displays the log of event buffers.
error	Displays the log of error buffers.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display the OTV log of events:

```
Router# show otv log event

[1 11/12/10 20:04:23.630 3] OTV-APP-DB: otv-app Database initializing (Overlay table size
= 4104 bytes (513 subblocks))
[2 11/12/10 20:04:23.630 3] OTV-APP-DB: Created otv_app subblock for overlay 1 VPN 1
[3 11/12/10 20:04:23.632 90] OTV-APP-EVC: Event: Walk topologies for VPN 0
3 entries printed
```

The table below describes the significant fields shown in the display.

Table 56: show otv log Field Descriptions

Field	Description
OTV-APP-DB	
OTV-APP-EVC	

Related Commands

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

show otv mroute

To display the Overlay Transport Virtualization (OTV) multicast route information from the Routing Information Base (RIB), use the **show otv mroute** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **mroute** [**bridge-domain** *bridge-domain-ID*| **vlan** *vlan-ID*] [**source** *source-address* **group** *group-address*]

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
bridge-domain *bridge-domain-ID*	(Optional) Displays multicast routes for the specified bridge domain. The range is from 1 to 4096.
vlan *vlan-ID*	(Optional) Displays multicast routes for the specified VLAN. The range is from 1 to 4094.
source *source-address*	(Optional) Filters output based on the specified IPv4 source address.
group *group-address*	(Optional) Filters output based on the specified IPv4 group address.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display multicast route information from the RIB:

```
Router# show otv mroute bridge-domain 289

OTV Multicast MAC Routing Table for Overlay1
Bridge-Domain = 289, s = 198.51.100.100, g = 232.1.1.20/8
 Incoming interface list:
  Overlay1, 198.51.100.100
 Outgoing interface list:
  Service Instance ID 50, GigabitEthernet 0/0/1
  Overlay1, 198.51.100.100
 Incoming interface count = 1, Outgoing interface count = 2

Bridge-Domain = 289, s = 198.51.100.101, g = 232.1.1.21/8
 Incoming interface list:
  Overlay1, 198.51.100.101
 Outgoing interface list:
  Service Instance ID 50, GigabitEthernet 0/0/1
  Overlay1, 198.51.100.101
```

```
 Incoming interface count = 1, Outgoing interface count = 2

2 multicast routes displayed in Overlay1
```

The table below describes the significant fields shown in the display.

Table 57: show otv mroute Field Descriptions

Field	Description
Bridge-Domain	The ID of the bridge domain where the multicast route was learned.
s	Source IPv4 address.
g	Group IPv4 address
Incoming interface list	The interface or Ethernet service instance where multicast packets are received.
Outgoing interface list	Interfaces or Ethernet service instances where multicast packets will be forwarded.

Related Commands

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

show otv route

To display Overlay Transport Virtualization (OTV) MAC routes from the Routing Information Base (RIB), use the **show otv route** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **route** [**neighbor-address** *neighbor-address*] [**bridge-domain** *bridge-domain-ID*| **vlan** *vlan-ID*] [*mac-address*] [**owner** {**bd-engine**| **isis**| **otv**}]

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
neighbor-address *neighbor-address*	(Optional) Filters output based on the specified IPv4 address of the neighbor.
bridge-domain *bridge-domain-ID*	(Optional) Displays unicast routes for the specified bridge domain. The range is from 1 to 4096.
vlan *vlan-ID*	(Optional) Displays unicast routes for the specified VLAN. The range is from 1 to 4094.
mac-address	(Optional) Filters output to display routes for the specified MAC address.
owner	(Optional) Filters output based on the specified owner.
bd-engine	Displays unicast MAC routes added by the BD-Engine. This keyword is available only when the **owner** keyword is configured.
isis	Displays unicast MAC routes added by Intermediate System-to-Intermediate System (IS-IS). This keyword is available only when the **owner** keyword is configured.
otv	Displays unicast MAC routes added by OTV. This keyword is available only when the **owner** keyword is configured.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display OTV MAC route information:

```
Router# show otv route

Codes: BD - Bridge-Domain, AD - Admin-Distance, SI - Service Instance
OTV Unicast MAC Routing Table for Overlay1
Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
0    67   67     0007.0007.0009 20    OTV    232.1.2.3
0    67   67     0102.0304.0506 40    BD Eng Gi0/0/1:SI67
0    99   99     0009.0009.0009 20    OTV    232.1.2.3
0    99   99     0038.0000.0000 1     OTV    Ov3, 10.33.1.0
0    99   99     0039.0000.0000 1     OTV    Ov3, 10.34.5.2
0    99   99     003a.0000.0000 1     OTV    Ov3, 10.35.4.6
0    99   99     003b.0000.0000 1     OTV    Ov3, 10.36.3.0
0    99   99     0102.0304.0507 40    BD Eng Et0/1:SI99

8 unicast routes displayed in Overlay1

OTV Unicast MAC Routing Table for Overlay2
Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
0    57   57     0005.0007.0009 20    OTV    Flood
0    57   57     0102.0304.0506 40    BD Eng Gi0/0/0:SI57
0    57   57     0102.0304.0508 40    BD Eng Gi0/0/0:SI57
0    57   57     0102.0304.0509 40    BD Eng Gi0/0/0:SI57
0    59   59     0005.0009.0009 20    OTV    Flood
0    59   59     0102.0304.0507 40    BD Eng Gi0/0/0:SI59

6 unicast routes displayed in Overlay2

OTV Unicast MAC Routing Table for Overlay3
Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------

0 unicast routes displayed in Overlay3

-----------------------------------------------------------
14 Total Unicast Routes Displayed
```

The table below describes the significant fields shown in the display.

Table 58: show otv route Field Descriptions

Field	Description
Inst	The OTV overlay instance.
VLAN	The VLAN that is advertised with the MAC address by IS-IS.
BD	The ID of the bridge domain where the MAC address was learned.
MAC Address	The learned MAC address.
AD	Administrative distance of the route. Routes with a lower administrative distance are preferred over routes with a higher administrative distance.
Owner	The component that added the route.
Next Hops(s)	Interfaces, Ethernet service instances, or remote OTV edge device where packets for this MAC address will be forwarded.

Related Commands

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

show otv site

To display Overlay Transport Virtualization (OTV) site information, use the **show otv site** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **site**

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays OTV site information such as the site bridge domain and neighbors within the site. If an overlay interface is specified, site adjacencies only in the same overlay are displayed. If the **all** keyword is specified, then even the site adjacencies that are not yet associated with an overlay are displayed.

Examples

The following example shows how to display all the OTV site adjacencies:

```
Router# show otv site

Site Adjacency Information (Site-VLAN: 1) (* - this device)

 Overlay1 Site-Local Adjacencies (Count: 2)

  Hostname       System ID        Last Change Ordinal    AED Enabled Status
* ED3            0026.CB0D.0800   2w0d        0          site overlay
  ED5            0026.CB0D.0801   1w5d        1          site overlay
```

The table below describes the significant fields shown in the display.

Table 59: show otv site Field Descriptions

Field	Description
Hostname	The dynamic hostname of the system.
System ID	The MAC address of the system.
Last Change	Time (in weeks, days) since the site adjacency last changed.

Field	Description
Ordinal	A zero-based value used for calculating the authoritative edge device (AED) for a VLAN.
AED Enabled Status	The IS-IS adjacency type used for determining AED status.

Related Commands

Command	Description
otv site bridge-domain	Configures a bridge domain for sending IS-IS hellos over site interfaces.
otv site-identifier	Configures a site identifier for an OTV site.
show otv isis	Displays the IS-IS status and configuration.

show otv statistics

To display Overlay Transport Virtualization (OTV) statistics, including some internal message counters, use the **show otv statistics** command in privileged EXEC mode.

show otv statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv statistics** command:

```
Router# show otv statistics

OTV App Statistics
 RIB route update messages sent: 30
  Success responses: 30
  Sys Limit Failure responses: 0
  Topo Limit Failure responses: 0
  Sys and Topo Limit Failure responses: 0
  Other Failure responses: 0
 RIB route delete messages sent: 27
  Success responses: 27
  Not Found Failure responses: 0
  Other Failure responses: 0
 RIB route lookup messages sent: 668
  Route found responses: 0
  Route not found responses: 668
  Failure responses: 0

 OTV App Event Count:
  Invalid event                      : 0
  Configured control-group           : 3
  Configured data-group              : 2
  Configured join-interface          : 2
  Configured ARP/ND suppression      : 2
  Configured active-source           : 59
  Configured fragmentation           : 1
  External interface address change  : 0
  Bridge-domain VLAN assigned        : 17
  Bridge-domain VLAN unassigned      : 0
  Request to walk topologies         : 2
  Request for topology VLAN          : 0
  Request to walk multicast mappings : 27
  AED change pending notification    : 26
  Delete feature data                : 0
  MLRIB event received               : 268
  Send MLRIB MAC flood update        : 0
  Send MLRIB redist registration     : 2
  First/Last Overlay event           : 1
  Tunnel repopulation request        : 0
```

```
Multicast HA DG sync               : 0
Multicast HA checkpoint mapping    : 0
ISIS mapping received              : 1263
ISIS overlay adjacency change      : 182
ISIS NSF mapping complete          : 0
ISIS NSF adjacency complete        : 0
Send MLRIB repopulation complete   : 0
MLRIB NSF redistribution complete  : 0
Join-interface OIR event           : 0
```

The table below describes the significant fields shown in the display.

Table 60: show otv statistics Field Descriptions

Field	Description
RIB route update messages sent	Total number of update messages sent to the MLRIB.
RIB route delete messages sent	Total number of delete messages sent to the MLRIB.
RIB route lookup messages sent	Total number of route lookup messages sent to the MLRIB.
OTV App Event Count	Number of OTV events processed by the system.

Related Commands

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

show otv summary

To display a table of all the Overlay Transport Virtualization (OTV) overlays configured on an edge device, use the **show otv summary** command in privileged EXEC mode.

show otv summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show otv summary** command:

```
Router# show otv summary

OTV Configuration Information, Site Bridge-Domain: 4

Overlay VPN Name        Control Group   Data Group(s)     Join Interface State
1       Northeast       225.22.22.22    232.5.0.0/8       Gi0/0/0        UP
2       Southwest       225.11.11.11    232.6.0.0/8       Gi0/0/1        DOWN
Total Overlay(s): 2
```

The table below describes the significant fields shown in the display.

Table 61: show otv summary Field Descriptions

Field	Description
Overlay	Overlay interface ID.
VPN Name	The OTV VPN name configured on the overlay interface.
Control Group	The IP multicast address used by OTV to form the overlay.
Data Group(s)	IP multicast addresses used for sending local IP multicast packets across the core.
Join Interface	The interface used for sending Internet Group Management Protocol (IGMP) joins towards the core.
State	The current state of the overlay interface.

Related Commands

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

show otv vlan

To display VLAN information for the Overlay Transport Virtualization (OTV) overlay interface, use the **show otv vlan** command in privileged EXEC mode.

show otv [**overlay** *overlay-interface*] **vlan** [**authoritative**]

Syntax Description

overlay *overlay-interface*	(Optional) Displays information about the specified overlay interface. The range is from 0 to 512.
authoritative	(Optional) Displays only authoritative VLANs.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If an overlay interface is specified, information for that overlay only is displayed; otherwise information for all overlays is displayed. When the **authoritative** keyword is specified, only those VLANs are displayed for which this device is the authoritative edge device (AED).

Examples

The following example shows how to display VLAN information for the OTV overlay interface:

```
Router# show otv overlay 1 vlan

Key:  SI - Service Instance
Overlay 1 VLAN Configuration Information
 Inst VLAN  Bridge-Domain  Auth  Site Interface(s)
 0    10    10             yes   Gi0/0/4:SI2
 0    11    11             yes   Gi0/0/4:SI3
 0    12    12             yes   Gi0/0/4:SI4
 Total VLAN(s): 3
 Total Authoritative VLAN(s): 3
```

The table below describes the significant fields shown in the display.

Table 62: show otv vlan Field Descriptions

Field	Description
Inst	The OTV overlay instance.
VLAN	The VLAN used by OTV when advertising local addresses.
Bridge-Domain	The ID of the local bridge domain associated with the given VLAN.

Field	Description
Auth	Authoritative status to indicate whether the edge device is authoritative and is forwarding traffic for the given VLAN.
Site Interface(s)	Interfaces and Ethernet service instances connected to the site network.

Related Commands

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

show parameter-map type waas

To display the parameter type configured for a Cisco Wide Area Application Services (WAAS) optimization, use the **show parameter-map type waas** command in privileged EXEC mode.

show parameter-map type waas *parameter-map-name*

Syntax Description

parameter-map-name	Name of the configured Cisco WAAS parameter map.

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 parameter-map type waas** command:

```
Device# show parameter-map type waas waas_global

parameter-map type waas waas_global
 tfo optimize full
 tfo auto-discovery blacklist enable
 tfo auto-discovery blacklist hold-time 60
 lz entropy-check
 no dre uplink
 accelerator http
   enable
   metadatacache enable
   metadatacache https enable
   metadatacache max-age 100
   metadatacache min-age 5
   suppress-server-encoding enable
 accelerator cifs
 accelerator ssl
    waas-ssl-trustpoint TP-self-signed-27050293
    cipher-list waas_global
    .
    .
    .
    services host-service peering
      version all
      peer-cipherlist waas_global
  enable
```

Related Commands

Command	Description
show policy-map type waas	Displays the policy map rules configured for a Cisco WAAS optimization policy map.

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
```

The table below describes the significant fields shown in the display.

Table 63: 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 policy-map type waas

To display the policy map rules configured for a Cisco Wide Area Application Services (WAAS) optimization policy map, use the **show policy-map type waas** command in privileged EXEC mode.

show policy-map type waas*policy-map-name*

Syntax Description

policy-map-name	Name of the configured Cisco WAAS policy map.

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 policy-map type waas** command:

```
Device# show policy-map type waas waas_global

Policy Map type waas waas_global
 sequence-interval 10
10 Class AFS
  optimize dre lz application Web
20 Class Http
  optimize lz application Filesystem
30 Class class-default
```

Related Commands

Command	Description
show parameter-map type waas	Displays the parameter type configured for Cisco WAAS optimization.

show platform hardware qfp feature otv client interface

To display Overlay Transport Virtualization (OTV) feature-specific information for the specified overlay interface, use the **show platform hardware qfp feature otv client interface** command in privileged EXEC mode.

show platform hardware qfp {**active**| **standby**} **feature otv client interface** *name*

Syntax Description

active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.
name	Name of the interface on which OTV is configured.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show platform hardware qfp feature otv client interface** command:

```
Router# show platform hardware qfp active feature otv client interface Overlay10

otv info:
  QFP interface handle: 8
  rx uidb: 245752  tx uidb: 245752
  config complete: False
  OCE type: Invalid
  oce_chain_p : 0x00010063
  Decap chain configured: True
  debug_flags : 0x0000ecaf
  ISIS Enabled: True
```

The table below describes the significant fields shown in the display.

Table 64: show platform hardware qfp active feature otv client interface Field Descriptions

Field	Description
QFP interface handle	An internal identifier assigned by the quantum flow processor (QFP) software for this interface.
rx uidb	An internal identifier for the receive side of the interface.

Field	Description
tx uidb	An internal identifier for the transmit side of the interface.
ISIS Enabled	Indicates whether or not IS-IS routing is enabled on the interface.

show platform software frame-relay

To display the statistics about frame relay permanent virtual circuits (PVCs), use the **show platform software frame-relay** command in the privileged EXEC mode.

show platform software frame-relay slot pvc [**interface interface**| **dlci number**]

Syntax Description

slot	(Optional) Embedded Service Processor or Route Processor slot. Valid options are: • F0—Embedded-Service-Processor slot 0 • F1—Embedded-Service-Processor slot 1 • FP—Embedded-Service-Processor • R0—Route-Processor slot 0 • R1—Route-Processor slot 1 • RP—Route-Processor
interface	(Optional) Indicates the specific interface for which PVC information will be displayed.
dlci	(Optional) Indicates the specific DLCI number used on the interface. Statistics pertaining to the specified PVC are displayed when a DLCI is specified. The valid value range is 16 to 1022.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Examples

The following is a sample output from the **show paltform software frame-relay rp active pvc** command displaying the forwarding manager frame relay PVC information:

```
router#show platform software frame-relay rp active pvc
Forwarding Manager Frame Relay PVC Information
Interface       DLCI        ID       QFP ID    Bandwidth  Fragm...
```

```
Serial0/1...      61      0x1020012      0          0          0
MFR1.1            100     0x1020013      0          0          0
```

show platform software l2fib fp

To display the global bridge domain table for MAC and Layer 2 multicast on the Forwarding Manager (FMAN) on Forwarding Processor (FP), use the **show platform software l2fib fp** command in privileged EXEC mode.

show platform software l2fib fp {**active**| **standby**} {**bd** *bridge-domain-ID* {**unicast** {**all**| **mac** *mac-string*}| **v4 group** {*group-addr* **source** *source-addr*| **all**}| **v6 group** *addr* {**all**| **source** *source-addr*}}| **mlist** {**index** *mcast-index*| **internal**| **summary**| **table**}}

Syntax Description

active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.
bd *bridge-domain-ID*	Displays information about the specified bridge domain. The range is from 1 to 100000.
unicast	Displays the Layer 2 Forwarding Information Base (L2FIB) unicast information.
all	Displays all MAC prefixes.
mac *mac-string*	Displays L2FIB MAC information for the specified MAC string.
v4 group *group-addr*	Displays IPv4 multicast group information for the specified group address.
source *source-addr*	Displays IPv4 multicast source information for the specified source address.
all	Displays all IPv4 prefixes.
v6 group *addr*	Displays IPv6 multicast group information for the specified group address.
all	Displays all IPv6 prefixes.
source *source-addr*	Displays IPv6 multicast information for the specified source address.
mlist	Displays an output list.
index *mcast-index*	Displays the specified multicast list platform index. The range is from 0 to 4294967295.
internal	Displays a management internals output list.
summary	Displays a summary output list.
table	Displays a table output list.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show platform software l2fib fp** command to display IPv4 multicast group information:

```
Router# show platform software l2fib fp active bd 10 v4 group all

Forwarding Manager L2FIB Mprefix Table

Prefix             Prefix Len       BD         Olist id         Prefix Id        Input If

-------------------------------------------------------------------------------------------
*, 224.0.0.0/0     4                10         0x7              0x24             0

*, 224.0.0.0/0     24               10         0xfa6            0x3ea3           0

*, 224.0.1.39/0    32               10         0xfa6            0x3ea4           0

*, 224.0.1.40/0    32               10         0xfa6            0x3ea5           0
```

The following is sample output from the **show platform software l2fib fp** command to display L2FIB unicast information:

```
Router# show platform software l2fib fp active bd 10 unicast all

MAC                         BD              Nhop type        Nhop Idx         Flags

ffff.ffff.ffff              10              olist            4006
```

The table below describes the significant fields shown in the display.

Table 65: show platform software l2fib fp Field Descriptions

Field	Description
Prefix	The IP multicast address in the *group-address*, *source-address* format.
Prefix Len	The prefix length the of the IP multicast address.
BD	The bridge domain ID.
Olist id	The multicast replication list ID.
Prefix Id	The platform ID allocated for the IP multicast prefix.
Input If	The input Ethernet Flow Point (EFP) for the IP multicast prefix.
MAC	The Ethernet MAC address.
Nhop type	The next hop type for the Ethernet MAC address.

Field	Description
Nhop Idx	The platform ID assigned for the next hop of the Ethernet MAC address.
Flags	Attributes associated with the Ethernet MAC address.

Related Commands

Command	Description
show platform software l2fib rp	Displays the global bridge domain table for MAC and multicast on the FMAN on RP.

show platform software l2fib rp

To display the global bridge domain table for MAC and multicast on the Forwarding Manager (FMAN) on the Route Processor (RP), use the **show platform software l2fib rp** command in privileged EXEC mode.

show platform software l2fib rp {**active**| **standby**}**mlist** {**index** *mcast-index*| **internal**| **summary**| **table**}

Syntax Description

active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.
mlist	Displays an output list.
index *mcast-index*	Displays the specified multicast list platform index. The range is from 0 to 4294967295.
internal	Displays a management internals output list.
summary	Displays a summary output list.
table	Displays a table output list.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show platform software l2fib rp** command:

```
Router# show platform software l2fib rp active mlist index 4006

L2FIB Mlist entries

Type  Index  AOM ID  CPP Info
efp   3ea1   OM:     0x42ad659c
oce   8f01   OM:     0x43877dc4
```

The table below describes the significant fields shown in the display.

Table 66: show platform software l2fib rp Field Descriptions

Field	Description
Type	The type of replication entries in the multicast replication list.

Field	Description
Index	The platform ID allocated for the multicast replication entry.
AOM ID	An internal object ID associated with the multicast replication entry.
CPP Info	The memory address allocated data-plane driver for the multicast replication entry.

Related Commands

Command	Description
show platform software l2fib fp	Displays the global bridge domain table for MAC and Layer 2 multicast on the FMAN on FP.

show platform software mfr

To display statistics about multilink frame relay information, use the **show platform software mfr**command in the privileged EXEC mode.

show platform software mfr slot {**active** [*counter*| *index*]| **standby**}

Syntax Description

slot	(Optional) Embedded Service Processor or Route Processor slot. Valid options are: • F0—Embedded-Service-Processor slot 0 • F1—Embedded-Service-Processor slot 1 • FP—Embedded-Service-Processor • R0—Route-Processor slot 0 • R1—Route-Processor slot 1 • RP—Route-Processor
active	Displays the active instance of the MFR.
counter	(Optional) MFR messaging counter information.
index	(Optional) MFR FP information pertaining to a specific index. The valid value range is 0 to 1000000.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Examples

The following is a sample output from the **show paltform software mfr fp active counters** command displaying the forwarding manager MFR message counters:

```
router#show platform software mfr fp active counter

Forwarding Manager MFR Message Counters
MFR Bundle additions         : 2
MFR Bundle deletions         : 0
MFR Bundle modifications     : 0
```

```
MFR Bundle errors            : 0
MFR Deferred Bundles         : 0
MFR Member Link additions    : 0
MFR Member Link deletions    : 0
MFR Member Link modifications: 0
MFR Member Link errors       : 0
MFR Deferred Links           : 0
```

show platform software otv fp

To display the overlay configuration on an Overlay Transport Virtualization (OTV) edge device on the Forwarding Manager (FMAN) on Forwarding Processor (FP), use the **show platform software otv fp** command in privileged EXEC mode.

show platform software otv fp {**active**| **standby**} {{**decap-oce**| **encap-oce**} [**index** *index*] **[all]**| **oce-stats**| **site-isis** *efp-dpidx*}

Syntax Description

active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.
decap-oce	Displays the OTV decapsulation object chain element (OCE).
encap-oce	Displays the OTV encapsulation OCE.
index *index*	(Optional) Displays the specified OTV decapsulation OCE platform index. The range is from 0 to 4294967295.
all	(Optional) Displays all entries starting from the specified decapsulation OCE index.
oce-stats	Displays OTV OCE statistics.
site-isis *efp-dpidx*	Displays the specified OTV site Intermediate System-to-Intermediate System (IS-IS) bridge domain Ethernet Flow Point (EFP) DPIDX (the internal platform index). The range is from 1 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show platform software otv fp** command:

```
Router# show platform software otv fp active encap-oce

Number of OTV Encap OCE entries in the table: 81

OTV Encap OCE: id 0x8f01, encap type MPLS_GRE, str 0x2a1ff
  Next OCE: type OBJ_ADJACENCY, id 0x8e25
  Overlay EFP: dpidx 0x10202de
  Flags: BCAST_PAK, STP_PAK, UNKNOWN_PAK
  Misc Info: CPP handle: 0x133dbe18 (om_id 65315 created)

OTV Encap OCE: id 0x8f02, encap type MPLS_GRE, str 0x2fb1ff
  Next OCE: type OBJ_ADJACENCY, id 0x8e25
  Overlay EFP: dpidx 0x10202df
  Flags: BCAST_PAK, STP_PAK, UNKNOWN_PAK
  Misc Info: CPP handle: 0x133e14b8 (om_id 65316 created)

OTV Encap OCE: id 0x8f03, encap type MPLS_GRE, str 0x2fc1ff
  Next OCE: type OBJ_ADJACENCY, id 0x8e25
  Overlay EFP: dpidx 0x10202e0
  Flags: BCAST_PAK, STP_PAK, UNKNOWN_PAK
  Misc Info: CPP handle: 0x133dbe50 (om_id 65317 created)
```

The table below describes the significant fields shown in the display.

Table 67: show platform software otv fp Field Descriptions

Field	Description
OTV Encap OCE	The OTV encapsulation Output Chain Element (OCE).
id	The platform ID allocated for OTV encapsulation OCE.
encap type	The encapsulation format.
str	The OTV encapsulation header.
Next OCE	The OCE following the OTV encapsulation OCE.
Overlay EFP	The platform interface ID for the Ethernet Flow Point (EFP) associated with the OTV encapsulation OCE.

Related Commands

Command	Description
show platform software l2fib fp	Displays the global bridge domain table for MAC and Layer 2 multicast on the FMAN on FP.